SERIE CRIPTOGRAFÍA - NOTA 1 DE 4 - CRIPTOANÁLISIS

NEX IT SPECIALIST #34



REVISTA DE NETWORKING Y PROGRAMACIÓN

#34

SECCIÓN ESPECIAL





OLPC ANALIZAMOS SU SISTEMA OPERATIVO

(EFS) ENCRYPTING FILE SYSTEM

TODAY´s CRYPTOGRAPHY

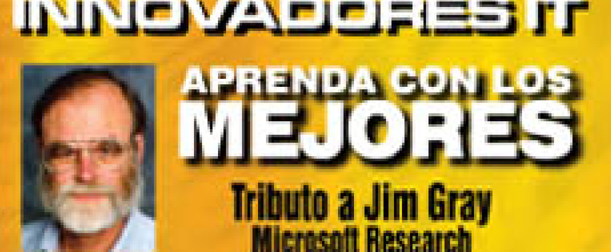
SERIE NETWORKING
QUALITY OF SERVICE
NOTA 1 - INTRODUCCIÓN Y CONCEPTOS

L2TP LAYER 2 TUNNELING PROTOCOL

TRIPLE PLAY
UNIFICACIÓN DE MEDIOS

FIRMA DIGITAL
PKI Y CERTIFICADOS DIGITALES

INNOVADORES IT



Tributo a Jim Gray
Microsoft Research

FIBRA ÓPTICA
EN COMUNICACIONES



- TODAY´S CRYPTOGRAPHY -

El proveedor está conectado al comprador regional
está conectado al canal
está conectado al sistema de administración de suministros
está conectado al código malicioso que justo ahora fue eliminado por la compañía líder mundial en seguridad empresarial.

Software de seguridad empresarial que logra interceptar las amenazas antes de que lleguen a usted. Software maligno. Usuarios malintencionados. Robo de información. El escenario de amenazas cambia cada día. Symantec le ofrece protección mundial 7x24 para proteger cada capa de su compañía: desde los dispositivos móviles al datacenter. Nuestros Servicios de Inteligencia Global están atentos a las amenazas emergentes para asegurarnos que su negocio se haye siempre protegido. **Si quiere saber mas sobre las mejores practicas de seguridad, descargue el With Paper:** **"Los elementos esenciales para la protección integral de los puntos finales".** *Visite www.symantec.com/offer e ingrese el codigo 37153*



Symantec Argentina. South of Latin America. Av. Alicia Moreau de Justo 1780 2ºF. (C1107AFJ) Buenos Aires, Argentina. (54 11) 4000-8787



DIRECTOR
- Dr. Carlos Osvaldo Rodriguez

PROPIETARIOS
- Editorial Poulbert S.R.L.

RESPONSABLE DE CONTENIDOS
- Dr. Carlos Osvaldo Rodríguez

DIRECTOR COMERCIAL
- Ulises Román Mauro
umauro@nexweb.com.ar

COORDINACIÓN EDITORIAL
- Carlos Rodríguez

SENIOR SECURITY EDITOR
- Carlos Vaughn O'Connor

EDITORES TÉCNICOS
- María Delia Cardenal
- Thomas Hughes
redaccion@nexweb.com.ar

DISEÑO Y COMUNICACIÓN VISUAL
- DCV Esteban Báez
- Carlos Rodríguez Bontempi

DISTRIBUCIÓN
distribucion@nexweb.com.ar

ASISTENTE DE MARKETING
- Juan Manzo

SUSCRIPCIONES
- Maximiliano Sala
- Ernesto Quirino
- Verónica Ruggieri
suscripciones@nexweb.com.ar

PREIMPRESIÓN E IMPRESIÓN
IPESA Magallanes 1315. Cap. Fed.
Tel 4303-2305/10

DISTRIBUCIÓN
Distribución en Capital Federal y Gran Buenos Aires: Huesca Distribuidora de Publicaciones S.A. Aristóbulo del Valle 1556/58. C1295ADH - Capital Federal Argentina. (www.distribuidorahuesca.com.ar)
Distribuidora en Interior: DGP Distribuidora General de Publicaciones S.A. Alvarado 2118/56 1290 Capital Federal - Argentina
NEX IT Revista de Networking y Programación
Registro de la propiedad Intelectual en trámite leg número 3038 ISSN 1668-5423
Dirección: Av. Corrientes 531 P 1 C1043AAF - Capital Federal
Tel: +54 (11) 5031-2287

Si desea escribir para nosotros, enviar un e-mail a:
articulos@nexweb.com.ar





Nota del Editor

Tributo

Hace 2 años conocí a Jim Gray en una conferencia especializada sobre base de datos y los sistemas de procesamiento de transacciones, ligada a los proyectos World-Wide Telescope, terraservice y skyserver. Aunque ya conocía su contribución en este campo, la presentación me hizo comprender la importancia de su trabajo. Hoy, desde "NEX IT Specialist", aún con alguna esperanza sobre su paradero, le hacemos un tributo a Jim.

Dr. C. Osvaldo Rodríguez*, Editor de NEX IT Specialist.*

Orgullo

La carta fechada 21 de Febrero 2007 leía:

"Estimado Dr. C. Osvaldo Rodríguez, nos es muy grato ponernos en contacto con usted en calidad de Presidente de la Asociación Hispanoamericana de Centros de Investigación y Empresas de Telecomunicaciones (AHCIET, www.ahciet.net) y de Cisco a fin de comunicarle:

Que el artículo "La tierra es plana, una oportunidad única para Latinoamérica" publicado en la Nex IT Specialist nº 27 ha sido ganador en primer lugar de la II Edición del Premio Periodístico AHCIET-CISCO "Pepe Cela".

Le ruego nos permita expresarle, en nombre la Asociación, de Cisco y en el nuestro propio, nuestra más sincera enhorabuena por el galardón al que se ha hecho acreedor.
Luis Di Benedetto, Presidente de AHCIET, **Alberto Arebalos**, Director de Comunicaciones para América Latina de Cisco.

Seguridad Informática y Criptografía

Seguridad informática está íntimamente ligada a la criptografía. Hoy, existen numerosas aplicaciones de gran utilidad centradas en criptografía. Cualquier aplicación típica con alto grado de complejidad estará construida sobre técnicas más básicas. Estas unidades más simples (básicas) son comunicaciones seguras, identificación, autenticación y cómo compartir secretos. Aplicaciones más complejas pueden incluir sistemas de comercio electrónico, certificación, correo seguro, recuperación de llaves y acceso seguro a una computadora.
La criptografía no está solamente confinada al mundo de las computadoras. Los teléfonos celulares la utilizan como medio de autenticación por ejemplo en verificar que un teléfono dado tiene el derecho de facturar una cuenta particular. La encriptación de la voz es usada para evitar que alguien externo a la comunicación pueda "escuchar" nuestra conversación.
Aunque en NEX ya hemos tratado diversos temas relacionados a la criptografía, a partir de NEX #34 comenzamos una serie de notas para entender esos pilares o técnicas básicas que permiten construir los sistemas más complejos. Las notas estarán a cargo de Pablo Anselmo quien, con absoluta claridad y compartiendo su experiencia profesional y docente, nos desarrolla la serie.
"NEX IT Specialist" #34 incluye como siempre, además de sus series, muchos otros temas interesantes.

No dejen de contactarnos a ***redaccion@nexweb.com.ar*** ●

LOS H

La confiabilidad que necesita

EDICIÓN ESPECIAL



Con Windows Server, Dattatec.com ganó en confiabilidad y creció 38% en 60 días

Luego de diversas pruebas, Windows Server demostró ser más confiable. **Pág. 15**

Desde sus inicios, Dattatec.com ofreció sus servicios en servidores Linux. Sin embargo, al incorporar la plataforma Windows a su oferta al mismo precio, más clientes lo eligieron por la confiabilidad de Windows Server.

Dattatec.com, firma regional de hosting de sitios web y aplicaciones online, logró reducir sus costos de operación y aumentar la confiabilidad y seguridad de sus servicios, alcanzando un crecimiento del 38% de su negocio en 2 meses.

La empresa trabajaba sólo con servidores Linux. Dada la cantidad de solicitudes recibidas y tras analizar el Microsoft Hosting Program, decidió incorporar una línea de aplicaciones y servicios de hosting sobre Windows. La confiabilidad de esta plataforma permitió a Datattec.com incrementar su volumen de facturación y cantidad de clientes, muchos de los cuales solían optar por otros proveedores que contaban con esa tecnología.

Ante las pruebas realizadas sobre un mismo hardware y con configuraciones similares, la plataforma Windows demostró soportar con un mejor rendimiento el doble de sitios que la platafomra de Linux.

"Entre sus servidores, Dattatec.com cuenta con uno dedicado para un diario online cuyo sitio esta desarrollado en Asp .Net y SQL Server el cual soporta actualmente más de 140.000 visitas diarias. En una oportunidad este servidor recibió un pico de 292.000 visitas en un día sin que su rendimiento se viera afectado", comenta Diego Vitali, director de Marketing de Datattec.com.

Por su parte, Guillermo Tornatore, CEO y fundador de la empresa, agrega: "A medida que avancemos en la implementación de la plataforma Windows, los costos de operación serán inferiores dadas las facilidades de administración y la flexibilidad para incorporar nuevas funcionalidades". "Sentimos un gran respaldo –asegura Tornatore– lo que nos da mucha seguridad para seguir creciendo. Microsoft es la plataforma que preferimos y recomendamos."

Continúa en Pág. 3.

Microsoft

ECHOS

para tomar sus decisiones

Para conocer más sobre este y otros casos visite http://www.microsoft.com/argentina/hechos
o llame al 0800-999-4617

FOTO: PEDRO GONZALEZ



En primera persona:

"Al sumar Windows Server 2003 encontramos una plataforma mucho más segura y confiable de lo que pensábamos. Demostró superar a Linux en escenarios de volumen y cumplió con todos nuestros requerimientos".

Guillermo Tornatore,
CEO y fundador de Dattatec.com

Confiabilidad récord

El aumento de la base de clientes de la empresa Dattatec.com confirma la preferencia del sistema Windows Server 2003 entre los usuarios más exigentes.
Pág. 8

Una compañía en crecimiento

Dattatec.com nació en el 2002 en la Argentina para proveer servicios de hosting de sitios web y aplicaciones online en América Latina. Está presente en Chile, México, Venezuela, España y los Estados Unidos. Tiene 60.000 sitios hosteados en cerca de 400 servidores.
Pág. 15

SUMARIO

NOTA DE TAPA

Today's Cryptograpy

22 - Criptografía - Introducción
28 - Encrypting File System (EFS)
34 - PKI - Firma Digital

Sección Especial Seguridad

12 **Security 2.0** - *Conozca la nueva integración de software, servicios y alianzas de Symantec.*

14 **Administración Global de Amenazas** - *Una solución de Symantec para protegerse contra los ataques de hoy en día.*



11

FOTO: (c) istockphoto.com/Andrey Prokhorov

RSA Conference 2007

Entre el 5 y el 9 de febrero se llevó a cabo en San Francisco uno de los eventos de seguridad más importantes: la RSA Conference 2007. Con 16 años de historia, la RSA Conference tiene como objetivo dar a conocer los temas más importantes de la seguridad dentro del mundo IT a más de 15.000 profesionales. El tema de este año fue la influencia de Leon Battista Alberti, creador del código polialfabético en la época renacentista.
En este contexto, el presidente de la RSA Security, Art Coviello (foto), predijo en la charla inaugural que en dos o tres años terminaría la autonomía de la industria de la seguridad, de aquellas compañías que ofrecen solo servicios de protección tales como antivirus o servicios de encriptación. "Nuestra industria está lista para una transformación. De hecho, ya se está llevando a cabo", expresó Coviello.
Dentro de la temática del discurso en el cual habló sobre la forma en la que la industria de la seguridad ha estado operando durante estos últimos años, Coviello argumentó que es necesaria una respuesta integrada para poder combatir las amenazas existentes para los usuarios de Internet y en los negocios.
Coviello resaltó que se espera que más de 200.000 nuevos virus aparezcan durante este año, lo que supondrá un gran desafío para la industria de los antivirus, y que los sistemas de prevención de intrusos solo están detectando el 70 por ciento de los ataques.
La solución, según Coviello, es preocuparse menos por los ataques individuales y hacer foco en asegurar que la información más importante se mantenga segura, quizás a través de una fuerte encriptación. Esto requiere que la información sea etiquetada y guardada de forma correcta. La próxima edición será entre el 7 y el 11 de abril de 2008 en San Francisco. ●

Para más info no dude en visitar *www.rsaconference.com/2007/US*





IDC Argentina Business Intelligence & Business Performance Management Conference

El 19 de abril se llevará a cabo la tercer edición del IDC Argentina Business Intelligence & Business Performance Management 2007. La agenda de la conferencia tendrá la presencia de un reconocido analista internacional de IDC quien presentará la visión mundial y tendencias de esta práctica.
El objetivo de este foro es dar a conocer a la audiencia dónde se encuentra hoy y hacia dónde va el mercado de BI. Mostrando el impacto del negocio con la adopción de estas herramientas, sus ventajas y beneficios actuales sobre esta tecnología. Se presentarán casos de éxito de empresas locales que adoptaron estas herramientas haciendo más productiva la operatoria diaria de su negocio.
Para más información visite: *www.idclatin.com/argentina* ●

CALENDARIO DE EVENTOS IT EN ARGENTINA PARA EL 2007

Fecha		Informes
	MARZO	
14	**Seminario Firma Digital - Price & Cooke**	www.pricecooke.com
15	**Segurinfo 2007** - Hotel Sheraton Buenos Aires	www.segurinfo.org.ar/
	ABRIL	
19	**Business Intelligence and Business Performance Management Conference** - Hotel Hilton Buenos Aires	www.idclatin.com/argentina
	MAYO	
15	**Dynamic IT: Infrastructure & Storage Vision Conference**	www.idclatin.com/argentina/
	AGOSTO	
2	**Business Mobility and Convergence Conference**	www.idclatin.com/argentina
	SEPTIEMBRE	
25	**IT Security and Business Continuity Conference**	www.idclatin.com/argentina

Si desea ver su evento IT publicado en esta sección, comunicarse a eventos@nexweb.com.ar

CeBIT 2007

CeBIT es el evento más importante de soluciones de telecomunicaciones y digitales tanto para el hogar como para los negocios. Esta exhibición, realizada todos los años desde 1986, cuenta con la organización de Deutsche Messe AG.
Este año se realizará entre el 15 y el 21 de marzo en Hannover. En estos días se presentarán keynotes de empresas como Microsoft, Siemens, Symantec y Software AG, quienes contarán sus experiencias y su visión del mercado en la actualidad y para el futuro.
Para más información visite la página oficial: *www.cebit.de* ●


Albé & Lamarche



Sección Especial Seguridad



Security 2.0

symantec™

Conozca la nueva integración de software, servicios y alianzas que ofrece Symantec para proteger la información.

El crecimiento del comercio en línea y de la variedad de formas en que es posible conectarse a Internet e interactuar en la red ha cambiado profundamente la vida de los consumidores, y también la de las empresas pequeñas y grandes que comercian con ellos. La forma en que trabajamos, vivimos, jugamos, compramos y nos comunicamos con amigos, familiares y colegas ha sufrido una transformación sin precedentes, tanto en su magnitud como en su velocidad de expansión. En un mundo interconectado, el factor armonizador que permite que todo funcione en conjunto es la confianza. La confianza que inspira seguridad. Esta confianza se genera cuando todos los participantes del mundo interconectados saben que su información está protegida, que sus interacciones son seguras y que los riesgos de sufrir daños son mínimos. Generar confianza en un mundo interconectado requiere un enfoque visionario. En Symantec, denominamos a este enfoque **Security2.0**.

Security2.0 no es un nuevo servicio o aplicación. Es la integración de software, servicios y alianzas que permiten proteger nuestra información, así como nuestras interacciones. El resultado: un entorno de productos, servicios y alianzas que ofrecen protección completa para todo tipo de entidades, desde clientes hasta empresas.

A medida que crece la Web, también crecen las oportunidades

Las innovaciones tecnológicas dan lugar a nuevas capacidades y modelos comerciales. Los clientes pueden conectarse directamente a las redes corporativas y efectuar transacciones que antes realizaban los empleados de la empresa. Las líneas que separaban a las empresas de los consumidores ya no son tan definidas, dado que las redes se han extendido e incluyen no solo a clientes sino también a empleados, proveedores y socios. Las transacciones entre distintas empresas, y entre empresas y clientes, están vinculadas por la apertura que permite la existencia del mundo interconectado. Las personas conforman el perímetro de la nueva red, que cambia constantemente para adaptarse a la naturaleza dinámica de las relaciones comerciales y a la creciente movilidad.

Nuevas fronteras y nuevas vulnerabilidades

Los clientes esperan un acceso más veloz a la información. También se espera que las empresas respondan rápidamente a las cambiantes demandas de los clientes y que, al mismo tiempo, busquen formas innovadoras de superar a los competidores de todo el mundo. Sin embargo, las amenazas externas como el phishing (suplantación de identidad), el pharming (reorientación del usuario a sedes virtuales falsas) y el robo de identidad se expanden a una velocidad cada vez mayor. Los criminales y los usuarios mal intencionados ya no se concentran en los equipos particulares o en las redes, ahora intentan alcanzar los niveles más profundos de los bancos de datos mundiales.

Estas alarmantes tendencias introducen nuevos riesgos para nuestro activo más valioso, la información, así como para nuestras interacciones, que en la actualidad abarcan docenas de plataformas y cientos de dispositivos. Las empresas también deben enfrentarse a amenazas de seguridad internas, como la fuga de información y los puntos finales no administrados. Los equipos portátiles, los PDA y los dispositivos Blackberry y Treo expanden el perímetro mediante el envío de información confidencial en todo momento, en cualquier lugar, a cualquier usuario.

Los riesgos de no cumplir con exigencias normativas y políticas de TI internas también son mayores. Al mismo tiempo, las compañías envían más información a su red extendida de empresas y efectúan transacciones de comercio electrónico complejas con varios participantes. Muchas empresas administran todas sus cadenas de abastecimiento en línea. Y cualquier cliente con una conexión a Internet puede llevar a cabo operaciones bancarias desde su hogar.

La protección de sus clientes y de la reputación de su empresa es fundamental.

Se ha demostrado en estudios que el 63 por ciento de las organizaciones esperan incurrir en un incumplimiento normativo importante y sufrir una pérdida de información significativa cada cinco años. El impacto de estos incumplimientos trae aparejado el daño a la reputación, la pérdida de ingresos y la pérdida de confianza por parte de clientes, socios e, incluso, accionistas.

La protección de la información es fundamental, pero no simple. Esto se debe a que la información no puede guardarse bajo las máximas medidas de seguridad; si es inaccesible, es inútil. Al mismo tiempo, si no está protegida, pasa a ser sospechosa o poco confiable.

La única respuesta para asegurar las interac-



ciones en línea son los productos y servicios integrados que construyen una visión global de la situación de seguridad de la organización. Soluciones que identifican los riesgos con anticipación, de forma que permitan mitigarlos y prevenir ataques. Ningún producto independiente puede ofrecer la protección que la gran diversidad de usuarios de Internet requiere en la actualidad, y en el futuro. Por eso Symantec está construyendo un entorno completo de productos, servicios y alianzas que ayudarán a crear un mundo interconectado seguro en el que los consumidores y las empresas puedan interactuar con confianza.

La confianza es el precio inicial del mercado

En última instancia, gracias a la protección de la información y las interacciones podemos desarrollar y solidificar la confianza y la seguridad, pasos esenciales para el funcionamiento del nuevo mundo interconectado. Cuando los consumidores sienten confianza, se sienten seguros para conectarse porque saben que su identidad estará protegida, que las personas con las que se comunican no son impostores y que los sitios con los que interactúan son legítimos. Cuando las empresas generan confianza, tienen más colaboración con socios y empleados, pueden ofrecer nuevos y convenientes servicios a sus clientes y, principalmente, se innovan y crecen de formas inesperadas.

En Symantec, nos esforzamos por generar confianza en un mundo interconectado. Como líder del mercado, nuestra misión es abrir camino hacia un futuro más seguro. Desde hace más de dos décadas, Symantec ha brindado protección para todos, desde usuarios individuales hasta empresas multinacionales. De hecho, protegemos a más personas de amenazas en línea que ningún otro en el mundo. Symantec se esfuerza por ofrecer las soluciones más innovadoras, que permiten a nuestros clientes estar protegidos y conectados, al mismo tiempo que pueden disfrutar de las emocionantes posibilidades que depara el futuro.

Symantec Security 2.0

Gracias a su desarrollo interno, a adquisiciones estratégicas y a alianzas, Symantec está en una posición única que le permite ofrecer soluciones completas e integradas que ayudan a proteger a nuestros clientes contra riesgos de seguridad. Nuestras poderosas soluciones son sólo el comienzo.

Symantec Global Services ofrece una experiencia y un conocimiento sin igual para ayudar a las empresas a equilibrar sus riesgos informáticos con la búsqueda de mayores ingresos comerciales. Con más de 900 profesionales de la asistencia y el respaldo de una red de servicio mundial de más de 2.000 personas, Symantec Global Services ofrece una amplia variedad de servicios de administración y evaluación de riesgos informáticos.

Nuestro programa de administración de amenazas y vulnerabilidades es el marco para procesar y priorizar la inteligencia de seguridad. Los servicios estables de consultoría ofrecen experiencia en seguridad a fin de aumentar las posibilidades de los usuarios. Los servicios de operaciones permiten deslocalizar las operaciones de seguridad según sea conveniente. Los servicios administrados de seguridad ofrecen control remoto ininterrumpido de firewalls, dispositivos de seguridad y sistemas de detección de intrusiones. Los servicios de advertencia temprana utilizan alertas personalizadas, análisis detallados y estrategias de mitigación para generar una vista completa de las amenazas de la red. Para las empresas, Symantec Enterprise Security Framework, el paquete de soluciones de seguridad más completo del sector, ayuda a proteger sistemas de punto final e información empresarial contra ataques maliciosos, robos y fugas. También ofrece administración de seguridad unificada en todos los niveles de la organización, de forma que las empresas puedan responder a todo tipo de desafíos de seguridad.

Ofrecer a nuestros clientes la confianza para trabajar y progresar en el mundo interconectado es más que nuestra tarea, es nuestra visión. Si quiere saber más sobre las mejores prácticas de seguridad, descargue el whitepaper “Los elementos esenciales para la protección integral de los puntos finales”. Visite www.symantec.com/offer e ingrese el código 37153. ●

Administración global de amenazas



Una solución de Symantec para protegerse contra los ataques de hoy en día.

La detención de ataques modernos requiere un planteamiento moderno de la administración de amenazas. Esto es exactamente lo que proporciona la administración global de amenazas de Symantec.

En lo que se refiere a la seguridad de la información de hoy en día, la mayoría de las organizaciones se encuentran en una situación poco sólida. En concreto, existen diferencias entre el nivel de protección que proporcionan sus medidas de seguridad y el nivel necesario para tratar adecuadamente la exposición a los riesgos.

A pesar de sus grandes esfuerzos, las empresas siguen siendo víctimas de ataques eficaces en proporciones alarmantes.

El problema principal es que las medidas defensivas concentradas en el perímetro que utilizan la mayoría de las organizaciones son incapaces de sostener el ritmo al que evoluciona el panorama de amenazas. Con más amenazas apareciendo y propagándose con mayor rapidez y efectividad que nunca, el resultado, en muchos casos, es un aumento continuo del caos. Además, parece que la financiación disponible (o al menos asignada) para corregir esta situación es relativamente escasa.

El panorama cambiante de las amenazas

Todavía son comunes los virus basados en archivos de movimiento relativamente lento y los gusanos de envío masivo. Sin embargo, un cambio en la motivación de los hackers, el deseo de conseguir notoriedad en lugar de ganar dinero y la creciente facilidad de acceso a estructuras del desarrollo de explotación son los factores principales que explican los cambios importantes surgidos en el panorama de las amenazas.

- El volumen de amenazas está aumentando.



El proveedor está conectado al comprador regional
está conectado al canal
está conectado al sistema de administración de suministros
está conectado al código malicioso que justo ahora fue eliminado por la compañía líder mundial en seguridad empresarial.

Software de seguridad empresarial que logra interceptar las amenazas antes de que lleguen a usted. Software maligno. Usuarios malintencionados. Robo de información. El escenario de amenazas cambia cada día. Symantec le ofrece protección mundial 7x24 para proteger cada capa de su compañía: desde los dispositivos móviles al datacenter. Nuestros Servicios de Inteligencia Global están atentos a las amenazas emergentes para asegurarnos que su negocio se haye siempre protegido. **Si quiere saber mas sobre las mejores practicas de seguridad, descargue el White Paper "Los elementos esenciales para la protección integral de los puntos finales"** . Visite *www.symantec.com/offer e ingrese el codigo 37153*





Symantec Argentina. South of Latin America. Av. Alicia Moreau de Justo 1780 2ºF. (C1107AFJ) Buenos Aires, Argentina. (54 11) 4000-8787

Aquí no hay ningún misterio. Una mayor motivación junto con menos barreras para desarrollar nuevos programas nocivos está conduciendo a un aumento en el número de las amenazas. Por ejemplo, en el primer semestre de 2005 se identificaron más de 10.800 nuevas variantes de virus y gusanos sólo para la plataforma Win32.

• El tiempo necesario para generar amenazas está disminuyendo. Otra consecuencia fruto de las complejas herramientas de los hackers ha sido el descenso del tiempo necesario para desarrollar una nueva amenaza.

• La velocidad de propagación de las amenazas está aumentando. Por ejemplo, en 2001 la velocidad de duplicación de la infección del Code Red fue de 37 minutos. Y en 2003, el gusano Sapphire duplicó su propagación cada 8,5 segundos, e infectó al 90 por ciento de todos los hosts susceptibles en menos de 10 minutos.

• Las amenazas se están haciendo más difíciles de localizar. Mediante mecanismos múltiples de desarrollo, cargas útiles y/o técnicas de propagación, las amenazas aumentan su potencial para eludir las defensas de las organizaciones y conseguir causar un impacto negativo.

Evidentemente, estos cambios tienen muchas e importantes consecuencias. En primer lugar, un mayor volumen de amenazas significa que habrá mayor presión sobre el personal de seguridad y sobre las medidas preventivas que se han implantado. Será necesario llevar a cabo una investigación más profunda que permita decidir cuáles son las amenazas más importantes, adoptar las medidas preventivas y resolver más sucesos e incidentes. A fin de restablecer el equilibrio, serán necesarios más administradores de seguridad o la implantación de herramientas que faciliten unas operaciones más eficaces, especialmente en lo que se refiere a actividades de investigación y mitigación.

Una segunda consecuencia es que la eficacia de la administración de parches como protección se reduce. En el pasado, el período que transcurría entre la aparición de una vulnerabilidad y su explotación era de varios meses, por lo que los fabricantes disponían de mucho tiempo para desarrollar y lanzar sus parches, y las empresas para probarlos e implantarlos. Sin embargo, en la actualidad, debido a que el período medio que transcurre entre la aparición de una vulnerabilidad y la publicación del parche correspondiente es de 54 días, existen muy pocas posibilidades de que haya un parche disponible a tiempo. Las organizaciones más eficaces, cuando trabajan en condiciones de emergencia, pueden conseguirlo en un par de días. Pero es mucho más frecuente que la ejecución rutinaria de un proceso de administración de parches de la empresa requiera un mínimo de 30 días.

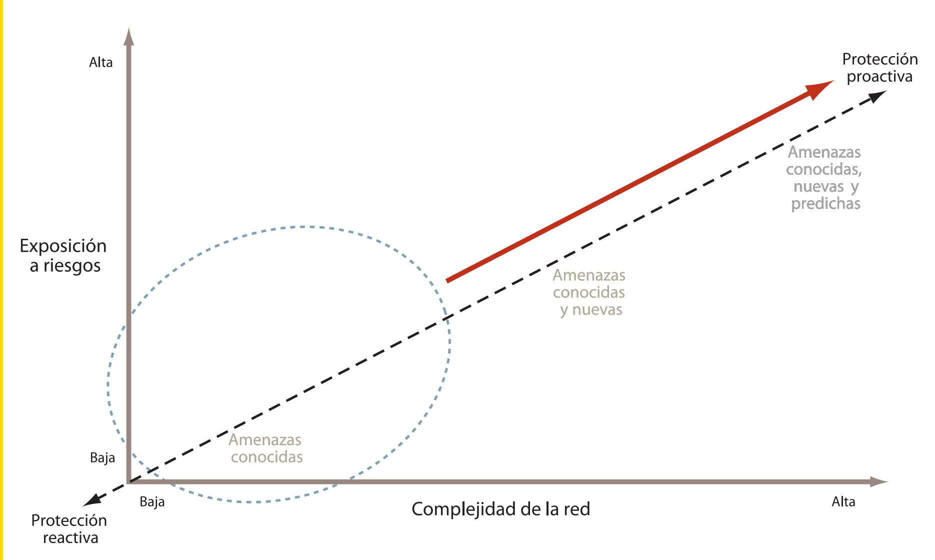


Fig.1 Protección contínua



Finalmente, el carácter esquivo propio de las amenazas modernas implica la necesidad de contar con defensas "combinadas". En otras palabras, además de medidas de prevención más proactivas, las organizaciones deberán incorporar a sus defensas una mayor variedad de mecanismos de detección, incluidos los que tienen mayor visibilidad a nivel de aplicación.

Factores agravantes

Por si el panorama actual de amenazas en continua evolución no fuese suficientemente problemático, existen varios factores relacionados que lo complican aún más.

• *El panorama de vulnerabilidades se está ampliando.* Debido a la necesidad de mantenerse competitivas, las organizaciones están adoptando nuevas tecnologías con mayor rapidez (por ejemplo, WLAN, VoIP, servicios Web), así como nuevas versiones de todos sus recursos existentes. El resultado es una población creciente de vulnerabilidades por defectos del código y mayores posibilidades de puntos débiles introducidos a través de errores y omisiones de configuración.

• *Las redes internas exigen atención.* La proliferación de conexiones de terceros, la necesidad de permitir a contratistas in situ conectarse a la red de la empresa y la creciente movilidad de los propios empleados están permitiendo a las amenazas burlar los controles de los límites de Internet para después propagarse, sin freno, desde el interior. Por consiguiente, las organizaciones están añadiendo redes y sistemas internos al conjunto de la infraestructura siempre creciente que necesita protección.

• *El cumplimiento normativo absorbe gran cantidad de recursos.* Otra de las razones que obliga a proteger las redes internas son las normas y legislación que exigen el cumplimiento de dichos aspectos. Sin embargo, el cumplimiento de estos requisitos es un problema si lo vemos desde la cantidad de recursos que consume y, en algunos casos, la falsa sensación de seguridad que proporciona.

• *Los presupuestos están sometidos a grandes presiones.* Basta decir que aunque los presupuestos de seguridad actuales no son irrazonables, no siempre se invierten de forma coherente con la reducción de los ataques y tienen que competir siempre con otras necesidades de la empresa.

La Necesidad: La administración global de amenazas

La posición de riesgo en la que se encuentran numerosas empresas de hoy día, empeorará si no se atiende debidamente. Contrarrestar esta tendencia exigirá a las organizaciones hacer inversiones adicionales en soluciones de seguridad de la información adecuadas. ¿Pero qué se puede considerar "adecuado" en este caso?

Parte de la respuesta a esta pregunta ya se ha revelado. De hecho, para que una solución resulte apropiada precisa de dos requisitos claros: que sea suficientemente proactiva, además de funcionar como pronóstico, y que proporcione una cobertura considerable (multinivel) del entorno informático, en lugar de centrarse solamente en los límites de Internet.

• *Proactivo* describe la capacidad de una

medida preventiva para bloquear una amenaza sin necesidad de saber explícitamente de qué se trata. Así, en lugar de depender de firmas específicas de amenazas, las medidas de protección proactivas utilizan mecanismos como la heurística, firmas basadas en vulnerabilidad y algoritmos de detección de anomalías. El grado adicional de protección que proporcionan permite a las organizaciones remediar vulnerabilidades de una forma más organizada.

Una medida preventiva también puede definirse como proactiva si proporciona alertas anticipadas de amenazas y vulnerabilidades, y permite a las organizaciones aplicar medidas atenuantes antes de que resulten afectadas.

Las medidas preventivas que llevan a este concepto un paso más lejos e intentan prever posibles amenazas podrían clasificarse como de pronóstico.

- *Multinivel* se refiere a la capacidad de una solución para brindar protección contra ataques en toda la organización y no sólo en el perímetro. Lo ideal es proporcionar cobertura a través de toda la red interna, en las conexiones de red a oficinas remotas, en estaciones de usuarios finales y en servidores importantes. Esto es necesario para obtener protección no sólo contra las amenazas que se originan en el interior, sino contra aquellas que eluden físicamente los controles del perímetro o que son capaces de atravesarlos. También es importante tener en cuenta que el planteamiento de "un solo tamaño adecuado para todo" no es apropiado.

Las características adicionales de una solución de seguridad adecuada que satisfaga las necesidades de protección contra ataques de las empresas no son exclusivas al problema que estamos tratando. Más bien, son las características ideales de cualquier solución de tecnología informática y deben ser eficaces, efectivas, flexibles y probadas.

La combinación de todas estas características sirve de base a un concepto que Symantec denomina "Administración Global de Amenazas". Esta solución de Symantec cuenta con los ingredientes necesarios para que las empresas resuelvan la discrepancia entre el nivel de seguridad y de protección contra ataques del que disponen y el nivel que realmente necesitan.

La solución: La administración global de amenazas de Symantec

Para Symantec, la administración global de amenazas no es tan sólo un concepto. La administración global de amenazas es una solución auténtica y a disposición de las empresas, cuyo objetivo es ayudarles a satisfacer su necesidad acuciante de disponer de un nivel de protección contra ataques eficaz y efectivo. Concretamente, incluye un conjunto de productos de seguridad de Symantec que se complementan con facilidad y que proporcionan funciones de administración de amenazas más amplias y detalladas. Los productos de la solución de administración global de amenazas incluyen Symantec Critical System Protection, Symantec Client Security y Symantec DeepSight Threat Management System, Network Access Control, Symantec On-Demand Protection Solution. Cada uno de estos productos incorpora un exclusivo conjunto de funciones líderes del sector y desempeña un papel específico dentro de la solución global.

symantec.
Proactiva y de pronóstico
Probada
Multinivel
Administración global de amenazas
Flexible
Efectiva
Eficaz

Fig.2 Características de una solución de administración de amenazas adecuada

Symantec Critical System Protection

Como se ha explicado anteriormente, los métodos y mecanismos de ataque actuales son mucho más complejos que nunca. Justamente para las "llegadas con éxito al sistema" se ha desarrollado un modelo de defensa fundamental para Symantec Critical System Protection. Utilizando políticas de seguridad basadas en comportamiento, Symantec Critical System Protection sólo permite buen comportamiento de sistemas operativos, aplicaciones, servicios y programas. Algunas veces, esto se denomina "endurecer el objetivo".

En muchas ocasiones, el código de explotación intentará sustituir un archivo del sistema existente por su propia versión modificada o añadir un código al registro del sistema para reinstalarse en el caso de que sea detectado. La polí-tica de seguridad principal de Symantec Critical Sys-tem Protection impide di-chos intentos. Las investigaciones realizadas por Sy-mantec han permitido esta-blecer que los daños causados por ataques a hosts se realizan casi exclusivamen-te mediante la modifica-ción de recursos del sistema que son de "sólo lectura" o que "no deben tocarse nunca".

A diferencia de otras herramientas de prevención de intrusos basadas en comportamiento, Symantec Critical System Protection crea políticas de seguridad para cada programa normal que se ejecuta en un sistema determinado. Gracias al editor de políticas incluido, la creación de dichas políticas es fácil y rápida, lo que permite una protección más granular y ayuda a eliminar falsos positivos, al tiempo que reduce la posibilidad de que se produzcan falsos negativos perjudiciales.

Symantec Client Security

Las mismas razones que requieren la protección de hosts críticos son aplicables a una población más alta de estaciones computacionales de usuarios finales menos críticas pero importantes. Además, ocurre que muchas plataformas cliente se ven expuestas con frecuencia a un mayor grado de riesgo al funcionar remotamente. Esto es debido a que en tales situaciones móviles, se carece habitualmente de la ventaja de los niveles añadidos del perímetro y de las medidas preventivas


La vulnerabilidad de su negocio
está conectada con la dimensión de su infraestructura de TI
está conectada con una adecuada evaluación de los riesgos involucrados
está conectada con las soluciones que gestionan la seguridad, disponibilidad y cumplimiento con normas
está conectado con Symantec Global Services para lograr resultados que se destacan, de principio a fin.
© 2006 Symantec Corporation.



basadas en red presentes cuando se trabaja en la LAN de la empresa. En cualquier caso, debe quedar claro que se trata de un procedimiento prudente que permite proporcionar a las plataformas cliente un conjunto fuerte de funciones de protección contra ataques. Aquí es exactamente donde entra en juego Symantec Client Security.

Al tratarse de un conjunto de tecnologías de seguridad integradas, Symantec Client Security permite a las organizaciones mantener el control de las estaciones de trabajo, reducir al máximo las interrupciones informáticas y mejorar la seguridad de los clientes. Se proporciona protección preactiva contra amenazas combinadas, spyware, acceso no autorizado a la red, gusanos de propagación masiva y una amplia variedad de otros tipos de amenazas.

Symantec DeepSight Threat Management System

Symantec DeepSight Threat Management System es una consola con todo tipo de funciones que permite recibir y revisar alertas anticipadas, estadísticas, análisis de expertos y consejos prácticos en relación con las nuevas vulnerabilidades y amenazas. Todo ello gracias a un recurso exclusivo y fundamental, la Symantec Global Intelligence Network. Mediante la ubicación de más de 20.000 sensores de sucesos en más de 180 países, junto con los diversos recursos públicos y confidenciales al servicio de cinco centros de operaciones de seguridad, once centros de soporte y seis laboratorios de respuesta de seguridad, Symantec recaba importante información sobre el panorama de amenazas y vulnerabilidades en continuo cambio. Un equipo de especialistas en seguridad altamente cualificados filtran y analizan los datos procedentes de esta red. Todos estos esfuerzos confluyen en un flujo confiable de información sobre alertas anticipadas en relación con vulnerabilidades y explotaciones recientemente descubiertas, ataques previstos y, lo que es más importante, asesoramiento activo para mitigación de amenazas y medidas preventivas asociadas. Además, la función de personalización permite a los administradores recibir únicamente la información relativa a su entorno específico de tecnología informática.

Proporciona información más inteligente y útil, mucho antes y con mayor eficacia de lo que sería posible en otras circunstancias y, de este modo, permite un nivel de protección proactiva contra ataques inigualable.

Pero ahí no queda todo. Symantec DeepSight Threat Management System también incluye un componente de pronóstico. Mediante la aplicación de diversas técnicas avanzadas de análisis a la información recopilada por Symantec Global Intelligence Network, los especialistas de seguridad de Symantec pueden identificar tendencias que potencialmente apuntan a nuevos ataques. El resultado es un grado de confianza aún mayor en donde la empresa no se verá afectada negativamente.

Symantec Network Access Control aumenta la seguridad y la disponibilidad de la red al permitir que la empresa imponga sus opciones de configuración de seguridad y de software en los host que están conectados a las redes empresariales. Soporte para la gran variedad de equipamiento de red, métodos de acceso y protocolos en la industria ayudan a que las organizaciones maximicen su ROI al eliminar las ataduras con los vendors específicos.

Symantec On-Demand Protection Solution ayuda a prevenir que el activo de su empresa, como el financiero o la información de sus clientes, se vea comprometido al no tener protegido el acceso a la red por aplicaciones web, LANs wireless, y SSL VPNs en dispositivos difíciles de manejar como las computadoras hogareñas y las laptops de invitados.

Conclusión

Es importante darse cuenta que la administración global de amenazas representa sólo una pequeña parte de la cartera de seguridad y disponibilidad global de la información de Symantec. De este modo, las empresas tienen la oportunidad no sólo de seguir mejorando la solución fundamental de la administración global de las amenazas (por ejemplo con la serie Symantec Security Information Manager), sino además de interrelacionarla con una estructura más amplia y más completa de soluciones de identidad, integridad, privacidad, confidencialidad y administración de la seguridad.

Si quiere saber más sobre las mejores prácticas de seguridad, descargue el whitepaper “Los elementos esenciales para la protección integral de los puntos finales”. Visite www.symantec.com/offer e ingrese el código 37153. ●

CRIPTO



Autor: **Ing. Pablo A. Anselmo**
Gerente de Seguridad Informática
Microsoft Cono Sur



FOTO: Google Blogoscoped - http://blog.outer-court.com/forum/27053-full.html

Hablar de Criptografía, pero en "español"

Cuando empecé a escribir este artículo recordé las veces que muchos de mis alumnos de la Universidad empezaron la cátedra de Seguridad Informática usando la expresión de que todo esto de la criptografía es "chino básico" y que para comprenderla hay que ser un experto en las matemáticas. Como estoy convencido que esto no es tan así, me puse el desafío de dar una introducción sobre la criptografía, su historia, su evolución y su actualidad, pero lo más en "español" posible.

La Criptografía es, sin duda, algo fascinante para algunos y un misterio para muchos; pero lo interesante tiene que ver con lo habitual que hacemos uso de estas técnicas criptográficas en nuestras vidas sin siquiera percibirlo. Por ejemplo: cuando hacemos uso del home banking, del cajero automático, de nuestras tarjetas de crédito, de nuestra contraseña para ingresar a la PC, de nuestro teléfono celular, cuando firmamos digitalmente un documento, cuando ciframos un correo electrónico, etc. Hay muchísimo para escribir sobre la Criptografía, pero como lo dije anteriormente; solo me limitaré a una introducción que sea lo más clara y sencilla posible.

Historia, origen y evolución de la Criptografía

La criptografía como conjunto de métodos y técnicas para cifrar (ocultar) un mensaje tiene sus orígenes en la Roma Antigua donde su significado en griego es "escritura oculta".
Julio César ya escribía textos cifrados (encriptados) para Cícero y para sus Generales hace más de 2000 años atrás; usando un algoritmo cifrador (que hoy lleva su nombre) donde cada

GRAFÍA

Introducción

letra era reemplazada por su siguiente en 3 posiciones más adelante en el alfabeto. **Ejemplo:** haciendo uso de este algoritmo, la palabra "Cesar" se escribe como "FHVDU" (sólo tenemos que reemplazar la "C" por la que le sigue en el alfabeto salteando 3 posiciones).

Tranquilos, que no todos los criptosistemas son así de sencillos y "Cesar" no es precisamente el que hoy le da seguridad a nuestras transacciones electrónicas. La evolución de la criptografía es muy amplia pero se destacaron en su historia sucesos como:

• El primer tratado sobre "Criptografía" fue escrito en 1518 por el monje benedictino Trithemius y se lo conoció como el libro "Polygraphia".

• Durante 1784 y 1789, Thomas Jefferson utilizó una "rueda criptográfica" (parecida al "criptex") para mantener comunicaciones privadas mientras representaba al Gobierno Francés (en esta época no había correo y toda la correspondencia era usualmente abierta y leída para ser vendida cuando tenía mucho valor).

• En la 2da Guerra Mundial, el secreto mejor guardado por los alemanes fue la máquina "Enigma", utilizada para proteger las comunicaciones entre el centro de mando y las tropas. Paralelamente a esto, en un remoto lugar llamado Bletchley Park un grupo de científicos, entre los cuales se destacaba Alan Turing, trabajan en el proyecto "ULTRA" que tenía como fin descifrar los mensajes enviados por los alemanes con la máquina "Enigma".

Finalmente, cabe aclarar que la criptografía ha tenido avances enormes en lo referente a su tecnología y complejidad; no obstante la política de tratamiento y divulgación de los algoritmos y sus avances fue tratado por muchos gobiernos como secretos militares. De



FOTO: Google Blogoscoped - http://blog.outer-court.com/forum/27053-full.html

hecho, en EEUU la NSA (Agencia Nacional de Seguridad) realiza fuertes inversiones en investigación y desarrollo de algoritmos de cifrado que son para uso interno del gobierno y no suelen someterse al análisis de la comunidad científica o académica mundial.

Otro aspecto a considerar son las restricciones políticas y legales que muchos países le han puesto a los algoritmos en nombre de la "seguridad nacional"; por ejemplo, en EEUU el software criptográfico está sujeto a las mismas leyes que las del tratamiento nuclear y los niveles de cifrado para exportar información o programas fueron hasta hace pocos años limitados a menos de 128bits.

Ahora bien, este tema de compartir los algoritmos no es menor, a lo largo de estos años si algo quedó claro es que la confianza que podemos depositar sobre un algoritmo de cifrado no está dado por otra cosa que por su sometimiento a la comunidad en general; para que sea analizado, probado (atacado) y evaluado en términos de seguridad, funcionalidad, eficiencia y robustez. El no operar bajo estos términos ha producido resultados lamentables ya que algoritmos como los primeros usados en la tecnología GSM fueron vulnerados en menos de 48hs.

Un algoritmo entonces será más confiable cuanto más tiempo lleve abierta su estructura en la comunidad científica sin lograrse obtener mediante el "Criptoanálisis" la clave secreta o el mensaje oculto.

Definiciones y otras formas de "cifrado"

Hasta ahora tratamos muy brevemente la historia de la criptografía y tocamos ciertos conceptos de manera ligera pero estratégica. Es decir, quise transmitirles aspectos de la historia y los usos de la criptografía para que puedan formar su propia idea de lo que significa.

Si tuve éxito, Uds estarán a estas alturas concluyendo que la criptografía tiene que ver con esto de **"proteger"** (seguridad) algo mediante el **"ocultamiento"** o **"distorsionamiento"** (técnicas de cifrado) de aquel **"elemento"** (mensaje) original para **"compartirlo"** (claves de cifrado) con otra **"parte"** (persona). Si esto es así, los felicito, porque palabras más o palabras menos, la ciptografía refiere sin duda a lo que Uds han podido concluir. No obstante a lo anterior, me permito citar la definición de la Real Academia Española sobre "Ciptografía": "...el arte de escribir mensajes con una clave secreta o de modo enigmático...".

Ahora, compartamos una definición algo más técnica que nos dará lugar a trabajar sobre otros conceptos: "...rama inicial de las Matemáticas y en la actualidad de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar un mensaje o archivo por medio de un algoritmo, usando una o más claves. Esto da lugar a diferentes tipos de criptosistemas que ayudan a asegurar cuatro aspectos fundamentales de la seguridad informática: confidencialidad, integridad, autenticación y no repudio de emisor y receptor".

Durante esta última definición quedaron evidenciados varios conceptos que quizás valga aclararlos antes de continuar. Por ello, a continuación hay algunas definiciones "lo más sencillas posibles" a considerar:

• **Método o técnica:** Es el proceso, generalmente matemático, utilizado para el cifrado o descifrado. Éste utiliza una lógica ("algoritmo") que suele ser la base de su fortaleza y una clave (o par de claves) que tienen por objeto "compartir" entre dos o más partes el secreto que nos dará acceso a lo que queremos "ocultar".

• **Estenografía:** Es cuando los métodos o técnicas utilizan una foto, una pintura, un dibujo, un documento, una planilla de cálculo, un archivo de texto o cualquier otro objeto digital para ocultar dentro del mismo el "mensaje original".

• **Otros métodos para ocultar información:** Escribir un mensaje dentro de otro, hallando las palabras que importan mediante un "criterio" (lógica del algoritmo + clave) que solo comparten los involucrados. Otro método conocido es el uso de una tinta especial para escribir un mensaje arriba de otro y que solo a partir de la reacción de ciertos químicos se podría leer. Finalmente, son también conocidos aquellos que aplican un relieve sobre las hojas de papel o bien tienen inscriptos una serie de puntos que guardan en sí al mensaje "oculto".

• **Criptoanálisis:** El criptoanálisis consiste en comprometer la seguridad de un criptosistema. Esto se puede hacer descifrando un mensaje sin conocer la llave, o bien obteniendo a partir de uno o más criptogramas (mensaje cifrado) la clave que ha sido empleada en su cifrado. No se considera criptoanálisis el descubrimiento de un algoritmo secreto de cifrado (código del algoritmo); ya que hemos de suponer que los algoritmos siempre son conocidos y abiertos.

Técnicas de Criptoanálisis

- **Texto plano elegido:** estudia grandes cantidades de pares **mensaje-criptograma** generados con la misma clave.
- **Ataque por fuerza bruta:** tratar de criptoanalizar un sistema aplicando el algoritmo de descifrado, con todas y cada una de las claves, a un mensaje cifrado que poseemos y comprobar cuáles de las salidas que se obtienen tienen sentido como posible texto original (texto plano).
- **Análisis diferencial:** partiendo de pares de mensajes con diferencias mínimas (usualmente de un bit), estudiar las variaciones que existen entre los mensajes cifrados correspondientes, tratando de identificar patrones comúnes.
- **Análisis lineal:** emplea operaciones XOR (OR exclusivo) entre algunos bits del texto plano y algunos bits del texto cifrado, obteniendo usualmente un único bit. Si realizamos esto con muchos pares de texto plano-texto cifrado podemos obtener una probabilidad p en ese bit que calculamos.
- **Por frecuencia y uso de letras:** cada lenguaje tiene la particularidad de utilizar con más frecuencia determinadas letras. Esto sirve de mucho ya que puedo saber qué letras utilizar primero en el ataque de fuerza bruta (porque es más probable que existan en el datagrama) o a partir de identificar que un digito se repite el mismo porcentaje de veces que una letra del alfabeto.

Ejemplo: En Inglés la letra **E** se repite en promedio unas 1231 veces, la letra **T** unas 959 veces, la letra **A** unas 805 veces, la letra **O** unas 794 veces, la letra **N** unas 719 veces, la letra **I** unas 718 veces, la letra **S** unas 659 veces, la letra **R** unas 603 veces, la letra **H** unas 514 veces, la letra **L** unas 403 veces, etc.

En las tablas 1 y 2 se puede ver un comparati-

vo entre los porcentajes de veces que se utilizan determinadas letras según el lenguaje.

Algunos conceptos interesantes de considerar antes de seguir:

• **Criptología:** Engloba Técnicas y métodos utilizados en Criptografía y Criptoanálisis.

• **Criptosistemas:** Es el proceso criptográfico en sí mismo, se lo puede entender de la siguiente manera.

Dado **M, C, K, E** y **D**; donde:

m = Mensaje a cifrar y **C** = Mensaje cifrado

K = Clave utilizada para cifrar o descifrar

E = Conjunto de transformaciones de "cifrado"

D = Conjunto de transformaciones de "descifrado"

$$Ek(m) = C$$

$$Dk(Ek(m)) = m$$

• **Secreto de un Sistema Criptográfico:** Fue definido por Claude Shannon y busca medir el nivel de secreto que tiene un "Criptosistema" a través del grado de "incertidumbre" que se puede tener al recibir un "Criptograma".

• **Secreto perfecto:** Un sistema tiene "Secreto Perfecto" (según C. Shannon) si el conocimiento del texto cifrado no proporciona ninguna información acerca del mensaje. Es decir, cuando la probabilidad de descubrir el mensaje plano o la clave a partir del mensaje cifrado es tendiente a 0 (cero).

• **Técnicas de "difusión" y "confusión":** Estas técnicas son utilizadas en muchos algoritmos muy conocidos, como ser DES, 3DES, etc. Para lograr un mayor secreto en las operaciones de cifrado Claude Shannon propuso usar dos técnicas:

- **Difusión:** es la transformación sobre el texto en claro con el objeto de dispersar las propiedades estadísticas del lenguaje sobre todo el criptograma.

Esto se logra a través del uso de las **"transposiciones"**: consiste básicamente en una **permutación**, es decir, cambiar los caracteres de lugar según una regla, una función, etc. Por ejemplo el carácter primero se posiciona en el lugar cuarto, el segundo en el lugar tercero, etc, etc. En el cuadro veremos un ejemplo de un mensaje que es cifrado y descifrado a partir de una palabra clave "COMPUTER" (ver cuadro); en la cual, el orden alfabético y ascendente de sus letras define la lógica de dicho algoritmo

- **Confusión:** es la transformación sobre el texto en claro con objeto de mezclar los elementos de éste, aumentando la complejidad de la dependencia funcional entre clave y criptograma.

Esto se logra a través del uso de las **"sustituciones"**, la cual consiste básicamente en modificar la información, es decir, sustituir un carácter por otro de acuerdo a una regla, una función, etc. Por ejemplo cambiar la letra A por la letra M, la letra B por la letra X , etc.

Criptosistemas

Los Criptosistemas se clasifican según el tipo de tratamiento que le dan el mensaje que van a cifrar:

A - Cifrado en "bloques"

Divide el mensaje a cifrar en N bloques de, por lo general, 8 bytes (64 bits) y los cifra de manera independiente (N bloques dependerá de la longitud del mensaje y x bits dependerá del algoritmo utilizado). En el caso de DES, divide los mensajes en bloques de 64 bits y los separa luego en 2 bloques de 32 bits cada uno (conocidos como Lo y Ro), luego realiza una "permutación inicial" y comienza la fase de cifrado a través de 16 vueltas en las cuales intervienen permutaciones y sustituciones (más adelante veremos con un poco más de detalle el proceso de cifrado del DES). **En las próximas páginas profundizaremos sobre esto.**

Ahora bien, según el tipo de clave que utilicen se clasificarán nuevamente en:

- **Cifrado con "clave secreta"** = Criptosistemas **simétricos.**

Existirá una única clave (secreta) que deben compartir emisor y receptor. Con la misma clave se cifra y se descifra por lo que la seguridad reside sólo en mantener dicha clave en secreto.

- **Cifrado con "clave pública"** = Criptosistemas **asimétricos.**

Cada usuario crea un par de claves, una privada y otra pública. Lo que cifra el emisor con una clave, lo descifra el receptor con la clave inversa. La seguridad del sistema reside en la dificultad computacional de descubrir la clave privada a partir de la pública. Para ello usan funciones matemáticas (hash) de un solo sentido (es decir, no tienen función inversa).

B - Cifrado en "flujo": cifra cada bits de manera individual.

Usa el concepto de cifrado propuesto por Vernam, que cumple con las ideas de Claude Shannon sobre sistemas de cifrado con secreto perfecto, esto es:

1) El tamaño de las claves posibles es igual o mayor que el tamaño de los mensajes.

2) Las claves deben ser equi-probables.

3) La secuencia de la clave sesión se usa una sola vez y luego se destruye (sistema one-time pad).

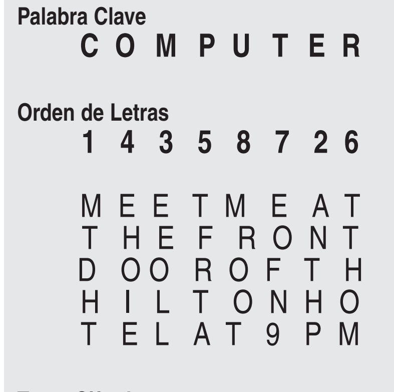
Las técnicas de cifrado en "flujo" consideran al menos:

- El mensaje en claro deberá leerse "bit" a "bit"

- Se realizará una operación de cifrado, usualmente a través de una función lógica "booleana" del tipo OR exclusivo (XOR) y con una secuencia cifrante de bits Si.

Ahora bien, en las próximas ediciones analizaremos solamente y con un poco más de detalle el CriptoSistema de "cifrado por bloques" y sus casos de "cifrado simétrico" y "asimétrico". ●

Cuadro



Texto Cifrado

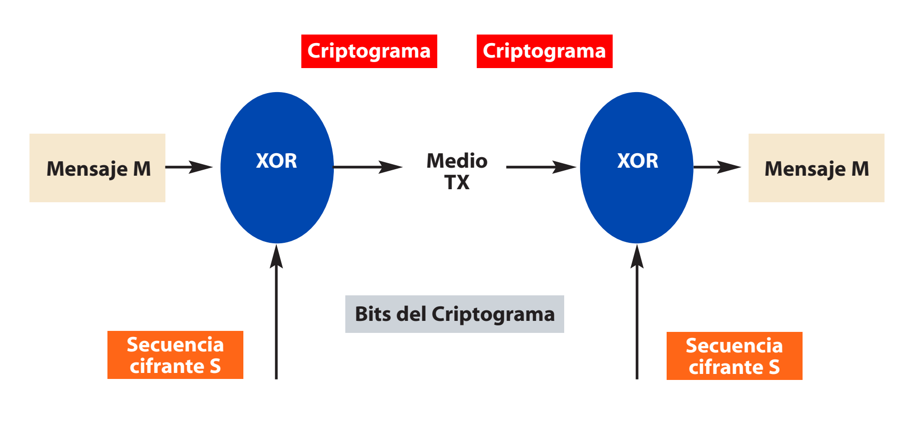
MTDHT ANTHP
EEOLL EHOIE
TFRTA TTHOM
EOFN9 MROOT

Texto Cifrado

Reunirte conmigo en el frente del Hilton a las 9PM!!!

Tablas 1 y 2

Vocales		LNRST	
Inglés	40%	Inglés	33%
Alemán	40%	Alemán	34%
Francés	45%	Francés	34%
Italiano	48%	Italiano	30%
Español	47%	Español	31%
Portugués	48%	Portugués	29%



EFS Recuperación de Datos y Sistema de Encriptación de Archivos

Autor: **Alun Jones**
MVP de Microsoft Security

Así que finalmente lo hizo. Marcó la casilla correspondiente para activar el Sistema de Encriptación de Archivos –o Encrypting File System (EFS)– en ese archivo que contiene información corporativa confidencial. A lo mejor se trata de números de cuentas bancarias de sus clientes, de información médica, o del plan súper secreto que su compañía elaboró para dominar el mercado. Cualquiera sea el contenido de este archivo, usted y su empresa decidieron protegerlo. Pero ahora la duda lo carcome: ¿qué garantía tiene de que podrá abrir nuevamente el archivo? ¿Está seguro de que podrá recuperar sus datos? Quizás en este preciso momento recuerde cuando aquella vez perdió la llave de un candado y debió romperlo para poder abrirlo. ¿Ahora también le sucederá lo mismo?

Es un hecho indiscutible que en nuestra era tecnológica existe la necesidad de recuperar datos aún cuando el responsable de haberlos encriptado no pueda hacerlo. Quizás esta persona esté enferma o de viaje, o quizás renunció en malos términos y usted no puede pedirle que recupere los archivos en cuestión. O quizás usted necesita recuperar archivos en el transcurso de una investigación sobre la sospechosa conducta de un usuario, y no quiere que su meta sea evidente.

Claramente existen buenas razones para que usted quiera estar seguro de que puede recuperar datos así como también protegerlos de algún acceso indebido. Este artículo presenta un rápido panorama de lo que necesita hacer para aprovechar el EFS de la mejor manera. Usted aprenderá sobre políticas y procedimientos, sobre agentes de recuperación de datos, sobre la realización de backups y la restauración de operaciones.



Preparandose para el Éxito

Con la clave en mano

Un primer llamado de atención sobre la instancia de preparación: antes de que sus usuarios encripten un archivo, pregúntese por el origen de las correspondientes claves de encriptación. Si no actúa en este sentido, las claves de encriptación serán generadas en forma aleatoria por cada usuario que encripte un archivo por primera vez, de tal manera que cada usuario obtendrá un certificado auto-iniciado y una clave de encriptación asociada. Para muchas organizaciones esto no es lo ideal, porque estas claves y certificados se encuentran descentralizadas y son difíciles de administrar y de backupear. Existe una solución mucho mejor que consiste en crear en su dominio una Windows Enterprise Certification Authority (WECA), y en configurar plantillas certificadas para certificados EFS, junto con una política de auto-registración. Los certificados de auto-registración admiten certificados de administración centralizada de usuarios, así como la posibilidad de archivar claves privadas, lo cual deposita toda la confianza en los agentes de recuperación de datos como único punto de recuperación.

Nota: Cada archivo protegido a través de EFS se encuentra encriptado, a partir de una clave generada en forma aleatoria y de un algoritmo de encriptación simétrico (esto supone un método de encriptación que utiliza la misma clave tanto para desencriptar como para encriptar archivos). Esta clave simétrica es entonces encriptada y almacenada una vez por cada usuario (y agente de recuperación de datos) que ha accedido al archivo, utilizando la clave pública de ese usuario. Esto significa que el sistema operativo actúa en nombre de un usuario que puede usar una clave privada para desencriptar la clave simétrica del archivo, y utilizar la misma clave simétrica para desencriptar el archivo.

Agentes de recuperación de datos

La recuperación de datos exige preparación. Afortunadamente EFS figura por default en Windows, con esa preparación incluida, ya que exige la intervención de un agente de recuperación de datos para cada archivo encriptado. Cada vez que usted encripta un archivo, Windows permite que alguna de las dos claves sirva para desencriptar el archivo nuevamente, más tarde. Una de las claves pertenece al usuario que encripta el archivo, de tal manera que el usuario pueda acceder nuevamente al archivo. La otra clave pertenece al agente de recuperación de datos y, tal como sucede con la clave del usuario, la clave y el certificado del agente de recuperación de datos pueden ser creados por medio de acciones de los administradores, o son creadas cuando se las utilice por primera vez.

Por principio, se define al agente de recuperación de datos para que sea la cuenta del administrador. En máquinas aisladas y en máquinas en red, la cuenta del administrador es la primera cuenta del administrador que controla el dominio.

En esta instancia entra en juego su propia preparación. Usted querrá estar seguro de que la clave privada para el agente de recuperación de datos no se encuentra disponible online, lo cual significa que la clave se almacena en un sistema puesto en marcha y ejecutado, conectado a su grupo de trabajo o dominio. La clave del agente de recuperación de datos debe ser trasladada offline y guardada en un dis-

quete o DVD, para estar seguros de que será utilizada únicamente cuando un proceso de recuperación se haya activado. Usted se verá tentado de asignarle alguna otra cuenta como la predeterminada para el agente de recuperación, pero esto no soluciona el problema básico, es decir, la presencia online de una clave privada rara vez usada para una operación importante.

Exportación y eliminación de una clave privada

Exportar y eliminar una clave privada para un agente de recuperación de datos (o cualquier otro usuario) es un proceso relativamente simple. Siga los pasos enunciados a continuación:

1. Inicie una computadora dentro de su grupo/dominio como cuenta de usuario para el agente de recuperación de datos.
2. Abra los snap-in de los Microsoft Management **Certificates**. Le conviene hacerlo mediante la ejecución de Certmgr.msc. También puede seguir los pasos descriptos a continuación:

- Ejecute MMC.exe
- En el menú **Archivo** haga clic en **Agregar/Eliminar Snap-in.**
- En el cuadro de diálogo **Agregar/Eliminar Snap-in** haga clic en el botón **Agregar**.
- Haga clic en los **Certificados** de la lista de snap-ins disponibles, y luego haga clic en el botón **Agregar**.
- En el cuadro de diálogo **diálogo Snap-in de Certificados** elija **Mi cuenta de usuario**, y luego haga clic en **Finalizar**.
- Haga clic en **Cerrar** y luego en **OK** para cerrar los otros cuadros de diálogo.

3. En el árbol **Raíz de Consola**, abra **Certificados – Usuario Actual**, abra **Personal**, y luego abra la carpeta **Certificados**.
4. En la lista de certificados desplegados en el panel derecho, elija el certificado que posee el nombre de usuario para el agente de recuperación de datos en las dos columnas **Publicado Para** y **Publicado Por**. Cuando estas columnas son iguales casi siempre indican que el certificado es un "certificado auto-iniciado". Verifique que la columna **Propósitos Previstos** lea "Sistema de Encriptación de Archivos", tal como muestra la figura 1.
5. Haga clic derecho sobre el certificado que desea exportar, señale **Todas las tareas**, y luego haga clic en **Exportar**, tal como muestra la Figura 1. Inmediatamente se abrirá el **Asistente para la Exportación de Certificados.**
6. Lea el texto explicativo de la primera página del asistente, y luego haga clic en **Siguiente**.
7. En la página siguiente, debajo de **¿Desea exportar la clave privada con el certificado?**, elija **Sí, exportar la clave privada**. Esto es importante, porque la clave privada es lo que usted desea backupear y eliminar en este proceso. Haga clic en **Siguiente** (ver figura 2).
8. En la página siguiente del asistente elija un formato donde exportar. Si elige correctamente exportar la clave privada para el certificado, el sistema le brindará una sola opción, **Intercambio de Información Personal**. Este formato de archivo también es conocido como archivo .pfx o PKCS#12. Existen tres casillas disponibles para elegir con este formato, tal como se muestra en la figura 3.
La primera casilla es irrelevante porque el certificado que usted está exportando es un certificado auto-iniciado que contiene todo el path de certificación. En cambio, tilde siempre la segunda casilla, **Activar la protección fuerte**, cuando exporte a un archivo .pfx. También debe tildar la tercera casilla, **Borrar la clave privada si la exportación es exitosa**, de tal modo que después de exportar el archivo .pfx, la clave privada para el agente de recuperación de datos sea eliminada del almacenamiento online de certificados. Esto evita que exista alguna posibilidad de desencriptación mediante el uso de la clave privada de un agente de recuperación de datos, pero no evita la encriptación con el mismo certificado.
Nota: Cuando exporte la clave privada y el certificado de un usuario, no borre la clave privada después de la exportación, o el usuario no podrá leer archivos encriptados con ese certificado. Mientras un agente de recuperación de datos será raramente convocado para que desencripte, la mayoría de los usuarios podrá encriptar y desencriptar sus archivos una y otra vez, como parte de una rutina diaria
9. Haga clic en **Siguiente**, y luego escriba y confirme la clave con la que desea encriptar el archivo .pfx (ver figura 4).
10. Haga clic en **Siguiente** y luego ingrese un path y un nombre para guardar el archivo .pfx.
11. Haga clic en **Siguiente**, verifique que el



Fig. 2 Eligiendo exportar la clave privada

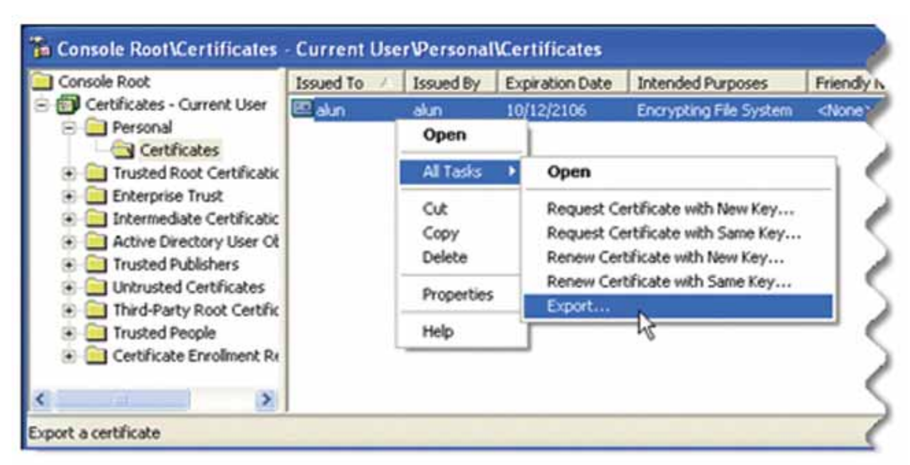


Fig. 1 Exportando la clave del Sistema de Encriptación de Archivos

resumen de operaciones encaja con lo que usted eligió, y luego haga clic en **Finalizar** para exportar su certificado EFS y su clave privada al archivo .pfx.

12. Guarde el archivo .pfx de manera segura. Mantenga buenos registros de la clave asociada al archivo .pfx (es recomendable hacerlo en una ubicación distinta de la utilizada para guardar el mismo archivo .pfx).

13. Asegúrese de contar a mano con un proceso apropiado para aprobar la confección del archivo .pfx y luego la clave, para cuando quiera importar la clave privada del agente de recuperación de datos. Así podrá recuperar documentos encriptados sin necesidad de recurrir a la clave privada del usuario.

¿Por qué querría usted exportar un certificado y una clave privada de usuario? En entornos anteriores a Windows 2000, una clave generada por el service desk impide que los usuarios accedan a sus certificados, porque éstos se encuentran encriptados a partir de una cadena de claves que se inician con el pasaporte del usuario. Aunque esto ha perdido vigencia en los entornos actuales, igualmente se recomienda que los usuarios técnicos realicen un backup de sus claves y certificados.

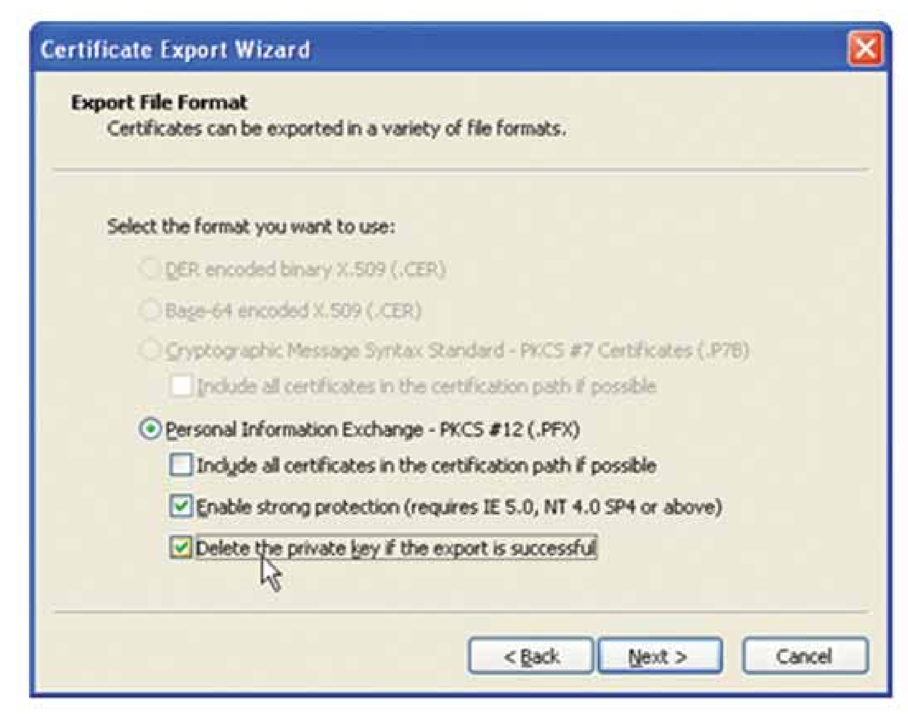


Fig. 3 Eliminando la clave privada después de la exportación

Brindando acceso adicional a un archivo encriptado

El agente de recuperación de datos es el primer intermediario en el proceso de recuperación de datos EFS. Desde ya, sumar usuarios para que accedan a un archivo puede ser otra manera de asegurarse la posibilidad de recuperar archivos cuando el usuario principal se encuentre ausente.

¿Cuál es la diferencia? Técnicamente, ninguna. Tal como lo apuntamos anteriormente cada usuario o agente de recuperación de datos posee una clave pública que puede servir para encriptar la clave de encriptación del archivo. De la misma manera, cada usuario del agente de recuperación de datos puede desencriptar el archivo utilizando su clave privada asociada para desencriptar la clave de encriptación del archivo. Sin embargo, desde el punto de vista administrativo, existe una gran diferencia. Usar la cuenta del agente de recuperación de datos para recuperar un archivo es una función administrativa, y sirve para un uso infrecuente cuando se recuperan archivos que de otro modo se perderían. Un agente de recuperación de datos es asignado a un archivo de manera administrativa, a través de una Política de Sistema de Encriptación de Archivos, y cuando esta política es fijada, se aplica al archivo encriptado. En cambio, agregar usuarios suplementarios a un archivo es considerada una función de usuario. Se espera que un usuario acceda regularmente a sus propios archivos, sin mediar un control administrativo u otro tipo de procedimientos formales. Como tal, ese usuario puede desear sumar a alguien más (por ejemplo a un asistente administrativo) a los archivos encriptados, de tal manera que ese usuario suplementario también pueda acceder a archivos encriptados como parte de su trabajo habitual.

Cualquier usuario que haya aceptado desencriptar un archivo EFS y que pueda reescribir el archivo, también puede agregar las claves públicas de otros usuarios para que accedan al archivo: en EFS no existe el concepto de un usuario especial que decide qué usuarios pueden ser agregados o eliminados, y acceder (o no) al archivo. Esto permite que una cantidad limitada de personas pueda acceder a un archivo. Lamentablemente, no hay manera de

asignar claves a un archivo desde un grupo de usuarios. Es posible acceder individualmente a cada clave pública de usuario, ya sea desde el almacenamiento local de certificados, o desde el servicio de directorios de Active Directory, para agregar el usuario al archivo. Desde una perspectiva criptográfica, ésta es una restricción necesaria, aunque puede resultar irritante cuando usted desea restringir un archivo a un grupo de usuarios. Recuerde que el sistema de protección de archivos NTFS puede resultar suficiente para archivos accesibles a un grupo, y que no todo archivo requiere una encriptación a través de EFS.

Cambiando su política EFS

El administrador de un dominio o empresa (o el administrador local de una red de computadoras o de una sola computadora) puede eliminar cualquier agente de recuperación de datos establecido por la Política del Sistema de Encriptación de Datos. Sin embargo, recomiendo vehementemente no hacerlo porque, en ese caso, es muy probable que termine perdiendo datos cada vez que el propietario de un archivo encriptado abandone su compañía, o cada vez que se desactiven claves o cuentas de usuarios. En cambio, es posible que a medida que su empresa crezca usted necesite seguir sumando agentes de recuperación de datos a la Política del Sistema de Encriptación de Datos. De todos modos recuerde que los cambios en esta política no afectan a los archivos ya existentes. De hecho, los cambios afectarán únicamente a los archivos creados o modificados bajo la nueva política. Se recomienda entonces mantener activos los archivos .pfx de un agente de recuperación de datos mientras los archivos EFS existan y sean utilizados por dicho agente.

Backup y Restauración

Como resulta imposible recuperar archivos que no cuentan al menos con una versión encriptada, asegúrese de que su software de backup almacene las versiones de archivos encriptadas con EFS. La mayoría de los productos comerciales para backup harán esto, por ejemplo el Backup de Windows o el Asistente de Restauración (NTBackup.exe), pero así y todo vale la pena verificar las capacidades de su software. Cuando el software exige abrir un archivo que ha sido encriptado con EFS desde una cuenta que carece de una clave privada asociada con ese archivo, el acceso es denegado. Su software de backup debe verificar específicamente los archivos que fueron encriptados con EFS; de lo contrario el backup de los archivos no se efectuará.

No ignore la manera más sencilla de recuperar datos: mantener un backup actualizado de los archivos más importantes, guardarlos en un gabinete seguro, todo en función de la confidencialidad de los datos involucrados. Obviamente, esto exige una actitud de cooperación por parte del propietario del archivo,



Fig. 4 Ingresando una clave contundente para el archivo exportado

que no debe ser tratado como el simple reemplazo de una buena política de recuperación. Como de costumbre, su herramienta de backup no será completamente aprobada si usted no controló el proceso de restauración de backups. Por lo tanto, evalúe si puede realizar el backup de un archivo encriptado, y también si puede restaurar el archivo en ambos casos, es decir, tanto si el propietario del archivo se encuentra disponible o si de lo contrario es necesario recurrir a un agente de recuperación de datos.

Esto me lleva a otro paso que usted puede dar para una recuperación de datos segura: poseer una "consola de recuperación central", una computadora que admita el ingreso de un agente de recuperación de datos para que restaure datos de backups, y para que luego desencripte archivos. Al restringir el desempeño del agente a una sola computadora, y al ubicar esta computadora en un área protegida, puede estar seguro de que la recuperación de datos quedará circunscripta sólo a aquellas ocasiones contempladas por sus políticas y procedimientos de recuperación de datos.

Conclusión

EFS puede dar miedo al principio y es cierto que efectivamente existe el riesgo de encriptar archivos de tal modo que sea imposible recuperarlos. Sin embargo, espero que este artículo haya servido para hacerle entender que basta con un poco de precaución y preparación para que sus archivos se encuentren disponibles únicamente para el personal debidamente autorizado. En definitiva, en ello radica todo este asunto de proteger sus archivos, ¿verdad? ●

Lecturas recomendadas

• *http://www.microsoft.com/technet/prodtechnol/win-xppro/support/dataprot.mspx*
"Protección y Recuperación de Datos en Win-dows XP". Este artículo proporciona una lista extensiva de links a información suplementaria.

• *http://www.microsoft.com/technet/security/tools/ cipher.mspx*
"Nuevas Herramientas de Seguridad para el Sistema de Encriptación de Archivos". Estos documentos descifran las líneas de comando de EFS.

• *http://support.microsoft.com/kb/223316/*
"Mejores prácticas para el Sistema de Encriptación de Archivos". Este artículo explica cómo agregar distintos usuarios y cómo realizar el backup de certificados de usuarios.

• *http://www.microsoft.com/technet/prodtechnol/winxppro/deploy/cryptfs.mspx*
"El Sistema de Encriptación de Archivos en Windows XP y Windows Server 2003". Este artículo proporciona detalles suplementarios sobre EFS.

** Este Artículo ha sido publicado en Microsoft Technet.*

PKI, FIRMA DIGITAL ¿Para todos y para todo?

Carlos Müller - Gerente Comercial - **Sitepro**

Dada la reciente publicación en el Boletín Oficial del decreto que establece el marco normativo sobre la Ley de Firma Digital en Argentina, han de resurgir sin duda muchos proyectos archivados y con ellos la necesidad de llevar a la práctica implementaciones de esquemas donde se utilicen Certificados Digitales para dar seguridad a distintas transacciones críticas, y para identificar a los actores que participen de las mismas.

La Ley de Firma Digital y su marco normativo son, sin duda, el puntapié inicial a tener en cuenta en todo proyecto de PKI (Public Key Infrastructure), pero hay que tener presente que el simple hecho de utilizar Certificados Digitales no es una "solución en sí misma", pues hay que contar con tecnologías adecuadas para proteger los Certificados Digitales contra ataques que puedan provocar el robo estas "identidades virtuales".

Está probado matemáticamente que los esquemas de PKI son seguros, siempre y cuando se mantengan protegidos los Certificados Digitales, la Clave Pública y la Clave Privada (esta última principalmente) de todas las partes que intervengan en dichos esquemas. De nada sirve utilizar claves de 1024 o 2048 bits si luego se terminan almacenando en la PC protegiéndolas con una simple password.

La Ley de Firma Digital en Argentina no "exige" ningún dispositivo especial para garantizar la seguridad de los Certificados Digitales, las Claves Públicas y Privadas de los usuarios, tal como lo hace la legislación chilena por ejemplo, que para lo que ellos denominan "Firma Digital Avanzada" (que se utiliza para operaciones bancarias, entre otras aplicaciones críticas) exigen el uso de dispositivos criptográficos que garanticen la generación y almacenamiento seguro del par de claves, sin posibilidades de que sea extraída de estos dispositivos la Clave Privada, es decir piden que se cumpla con la Norma FIPs 140-2 Nivel 2.



En la Argentina, en cambio, sólo se plantea que "los certificadores licenciados deberán informar a todo solicitante, previo a la emisión de los correspondientes certificados, la política de certificación bajo la cual serán emitidos, sus condiciones y límites de utilización, condiciones de la licencia obtenida y todo aquello que fuere relevante con relación a un uso correcto y seguro de dichos certificados".

Lo que sí queda claro en la Ley Argentina es la "exigencia" de la protección de las "claves raíces" de las "Autoridades de Registro o Certificantes", donde se requiere el uso de dispositivos criptográficos para su "generación y almacenamiento", que cumplan con la Norma FIPs 140-2 Nivel 3, siendo para ello necesaria la implementación de dispositivos

HSM (Hardware Security Module) como los LUNA SA de Safenet. Lo que sin duda implica importantes inversiones para cumplir con este requisito y otros que tienen que ver con el "acceso fisico" a los lugares donde se encuentren estos dispositivos y los servidores principales involucrados en los esquemas de PKI.
Es importante entender que para poder "ampararse" en la Ley de Firma Digital se deben cumplir todos sus requisitos, y sin duda esto difícilmente se logre en un cien por ciento, aún luego de pasado el tiempo suficiente para que se logre ir depurando los detalles poco claros que existen en toda nueva tecnología.
También hay que tener en cuenta que en toda implementación de seguridad existen distintos niveles de requerimientos, y por lo general para la mayoría de los usuarios es suficiente implementar soluciones alternativas mucho más simples y menos costosas, y sólo para un grupo reducido, que realiza las operaciones más críticas, sería necesario utilizar mayores niveles de seguridad. Y tal como ha dicho Carlos Achiary, Director de la ONTI (el organismo responsable de PKI en la Argentina), en una nota periodística, "la firma digital hay que usarla donde es necesaria porque agrega complejidad" y "como toda medida de seguridad es cara e incómoda".
Adicionalmente a todo lo expuesto hay que ser concientes que nada ha cambiado la realidad de Argentina, y Latinoamérica en general, sobre la falta de presupuesto para implementar esquemas costosos como los de PKI, y por lo general los proyectos que utilizan estas tecnologías al ser elevados por la gente de seguridad informática a los directivos de las empresas, o a la gente que manejan las finanzas, terminan en un "mejor dejemos este gasto para el siguiente presupuesto", pues nadie lo ve como lo que es realmente, una inversión.
Por ello para ciertas soluciones donde la escala del proyecto no permita amortizar la inversión necesaria para montar un esquema de PKI, no se debe olvidar analizar otras alternativas más "viables" para nuestra realidad regional, y entender que es preferible no seguir usando "usuario y password" mientras nos aprueban el presupuesto de inversión para estas tecnologías, y avanzar lo antes posible con otras alternativas que nos permitan estar mejor posicionados y no dejar siempre para el mañana todos los proyectos de seguridad que existen en nuestras empresas.
En la gran mayoría de las instalaciones o aplicaciones donde se necesita una "validación fuerte de acceso de usuarios", se puede implementar un "acuerdo entre partes" respecto a los elementos que se utilizarán para esta validación, con lo cual se podría optar por las opciones más simples de implementar y de menor costo, pues lo más importante, en definitiva, es este "acuerdo entre partes" que se va a firmar. ●

Links Relacionados

Link sobre la Normativa:
http://infoleg.mecon.gov.ar/infolegInternet/verNorma.do?id=125115
Link con Texto Completo:
http://infoleg.mecon.gov.ar/infolegInternet/anexos/125000-129999/125115/norma.htm
Link a los ANEXOS:
http://infoleg.mecon.gov.ar/infolegInternet/anexos/125000-129999/125115/decadm6-2007-anexo.pdf

Quality of Service en redes IP

INTRODUCCIÓN

Autor: **John William Graue**
Ing. en Electrónica **(UBA)**

Hablar de calidad de servicio (QoS) en términos de redes significa identificar y clasificar los distintos tipos de tráfico que tiene dicha red y darle trato diferencial a cada uno de ellos.

Serie - Nota #1 de 5

- **1: Introducción y conceptos de QoS**
- 2: Identificadores de QoS
- 3: Mecanismos utilizados en QoS
- 4: Manejando la congestión
- 5: Compresión

Redes convergentes

Antes de comenzar a leer el término "redes convergentes" en revistas especializadas, y que estas fueran ofertadas por los distintos Carriers, las empresas utilizaban distintos medios para cada uno de sus tipos de tráfico. La telefonía era transportada a través de la PSTN (Public Switched Telephone Network) mientras que se contrataba un servicio aparte para el transporte de los datos, típicamente uno de Frame-Relay.

En el caso del video es más complicado aún ya que para servicios de capacitación a distancia, por ejemplo, se necesita una red punto-multipunto teniendo que recurrir a un medio tipo broadcast como lo es el aire. Esto traía como consecuencia la contratación de un servicio satelital muy poco accesible para la mayoría de las pymes en términos monetarios. Por lo tanto sí o sí debían ser contratados con líneas separadas siendo ésta el tercer tipo de enlace contratado.

Con la aparición del transporte de la voz sobre IP (VoIP) las empresas comenzaron su implementación utilizando el mismo proveedor que utilizaban para los datos, haciendo converger dos tipos de tráfico con características distintas en un mismo enlace físico. Así nace el término "redes convergentes" y comienza a hacerse cada vez más fuerte con la mejora de la tecnología que rodea la voz sobre IP y fundamentalmente con la disminución del precio del ancho de banda ofrecido por los Carriers. Sin embargo, en la mayoría de los casos se utilizaba solo para la comunicación interna de la empresa, teniendo que utilizar otro aparato telefónico para llamadas hacia la PSTN o bien tener instalada una PABX que integrara las líneas "públicas" y "privadas".

Con la implementación de los softswitch por parte de los Carriers, apareció la posibilidad de dar Telefonía IP utilizando ahora el mismo enlace para todos los servicios y con acceso a la PSTN. En la figura 1 se puede ver un esquema que compara las dos formas de transportar los distintos tipos de tráficos.

Tipos de Tráficos

Como se mencionó anteriormente, las características de cada uno de los tráficos a ser cursado por

“El tipo de flujo clasificado como "datos" es todo aquel tráfico que puede ser retransmitido”

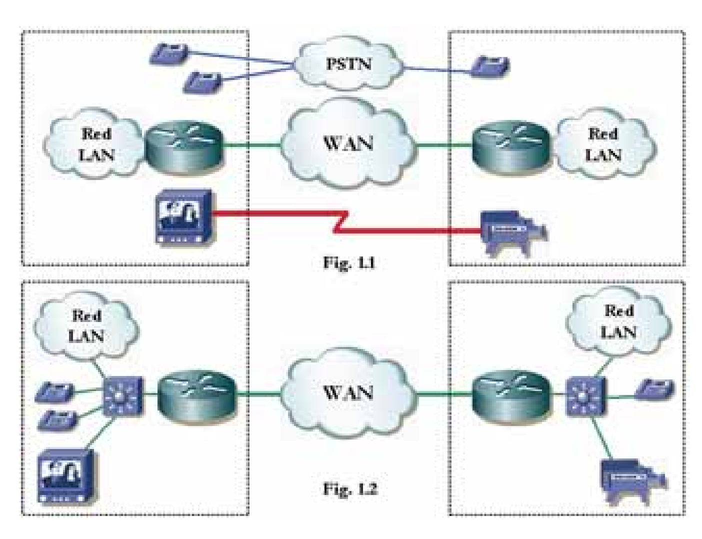


Fig.1 Forma de transportar distintos tipos de tráfico

el mismo vínculo son muy diferentes. El tipo de flujo clasificado como “datos” es todo aquel tráfico que puede ser retransmitido. Tales son los casos de los e-mails, la navegación Web, transferencia de archivos, etc. El protocolo utilizado en la capa de transporte para estos casos es generalmente TCP, el cual provee un mecanismo de detección de errores y pérdida de información que brinda la posibilidad de la re-transmisión de aquellos paquetes perdidos o erróneos. Por otro lado el flujo clasificado como “real time” es todo aquel que utiliza UDP como protocolo y que por ende no dispone de retransmisión de paquetes. Es por eso que un paquete de voz o video digitalizado no se retransmite bajo ninguna condición. Otra característica que los diferencia es la frecuencia de transmisión o constancia en que los paquetes deben ser transmitidos. Si el envío de paquetes no es constante en un flujo de video o voz se percibiría un corte en la imagen o audio respectivamente. Por ende, los paquetes no pueden esperar a ser transmitidos teniendo estos que ser atendidos de manera inmediata. Si una página tarda más en cargar en el navegador elegido, un email se demora un segundo más o menos, o el tiempo de transferencia de un archivo es levemente diferente a la vez anterior, son variaciones que no pueden ser percibidas por el usuario. Y si así lo fuera, no sería tan grave como el entrecorte de un servicio “real time”.

El tamaño de paquete es también diferente entre estas dos grandes clasificaciones de tráfico. El flujo “real time” es conformado por paquetes pequeños mientras que los de “datos” pueden ser mucho más grandes teniendo esto consecuencias grandes que serán explicadas en artículos posteriores.

A modo de ejemplo un paquete de “datos” puede ser de un tamaño de hasta 1500 Bytes en redes Ethernet mientras que uno de “voz” tiene un tamaño aproximado de 60 Bytes sin contar el encabezado del nivel 2.

Utilizando el Codec G.729 8bits (uno de los más populares en VoIP) a modo de ejemplo, se puede ver que:

La frecuencia de muestreo de la voz es de 8KHz, cada muestra se digitaliza en 8 bits, y se juntan 20 muestras en un paquete. Eso da un tamaño de payload de 20Bytes.

Tamaño de paquete: 20B Payload + 12B de RTP + 8B de UDP + 20B de IP = 60Bytes

Trato preferencial

Para tener una Calidad de Servicio (QoS) garantizada es de vital importancia el trato preferencial que se pueda tener con los paquetes de un tráfico “real time” con respecto al de los “datos”. Ese plus logrado en el trato será la clave del éxito de las implementaciones de las redes convergentes.

Aspectos claves

Ancho de banda recurso finito: teniendo un solo enlace físico para poder brindar los distintos servicios, hará que los paquetes de cada uno de ellos compitan por el ancho de banda (BW) contratado. Esto provocará que el uso del enlace por parte de uno de los tipos de tráfico reste BW para el otro. Teniendo que tener cuidado de tener reservado un porcentaje del mismo para el “real time” en caso de que este lo requiera, mientras que pueda ser utilizado por los “datos” cuando no exista una comunicación de voz ni video.

End-to-end Delay: el delay es un aspecto sumamente importante ya que es el retardo que un paquete de voz sufre desde que se generó en el equipo que digitalizó la misma hasta la llegada en el equipo destino. Más que un retardo constante, el peor enemigo de la calidad de voz es el Jitter (o variación del delay). Mientras que un delay constante provoca un retardo en la escucha del interlocutor, el Jitter provoca una deformación de la palabra que la vuelve inteligible.

Los tres factores que contribuyen al end-to-end delay (o retardo total en el enlace) son el tiempo de propagación del enlace, el retardo por serialización, y el de procesamiento y/o encolado (Queuing).

Todo medio de transmisión (aire, fibra óptica, par de cobre, etc.) posee un tiempo de propagación característico, y que es inevitable.

El retardo por serialización es el tiempo que el

“Cada uno de los bloques tiene que tener implementado QoS para dar tratamiento especial a cada tipo de tráfico”

equipo de transmisión tarda en “poner” el paquete en el enlace. Supongamos que un router tiene un vínculo de 256Kbps y que tiene que transmitir un paquete de 1000Bytes (8000 bits). El equipo tardará 31,25 ms en transmitir el paquete utilizando una regla de tres simple.

El tiempo que tarda un router en procesar el paquete (lookup de la IP destino por ejemplo) y el tiempo que el paquete permanece en los buffers de salida esperando a ser transmitidos también deben ser tenidos en cuenta en el end-to-end delay.

Pérdida de paquetes: uno de los mayores causantes de la pérdida de paquetes (sin tomar en cuenta los microcortes que se pueda tener a nivel físico) es la congestión del enlace. Si bien una buena práctica es reservar ancho de banda para el flujo “real time” y que este no se vea afectado con la presencia de alto tráfico de datos, ¿qué pasa si la suma de los dos flujos comienza a ser cercano al enlace físico? La respuesta es simple y es pérdida de paquetes. Para los casos en que la suma de los dos tipos de tráfico empieza a ser comparable con el enlace físico, se emplea un mecanismo que “castiga” al tráfico de datos, haciendo que este disminuya temporalmente. Ese mecanismo será detallado en artículos posteriores.

Asegurando la calidad del Servicio QoS

Las redes convergentes analizadas desde el punto de vista del Carrier se pueden dividir en los siguientes bloques:

Casa de cliente: dentro de la casa de cliente se encuentra la red o redes locales (LAN) que tienen como punto de salida hacia la red del Carrier el CPE (Customer Premise Equipment) del mismo.

Red de Acceso: la red de Acceso es la que comunica un CPE con el Backbone del Carrier. Para VPNs de nivel 2 implementada con Frame Relay, la red de Acceso es la capa de transporte (nivel 1) que da conectividad con el Switch Frame Relay ubicado en el nodo del Carrier. Por lo general son redes PDH, SDH o Wireless (ya sea punto a punto o punto-multipunto).

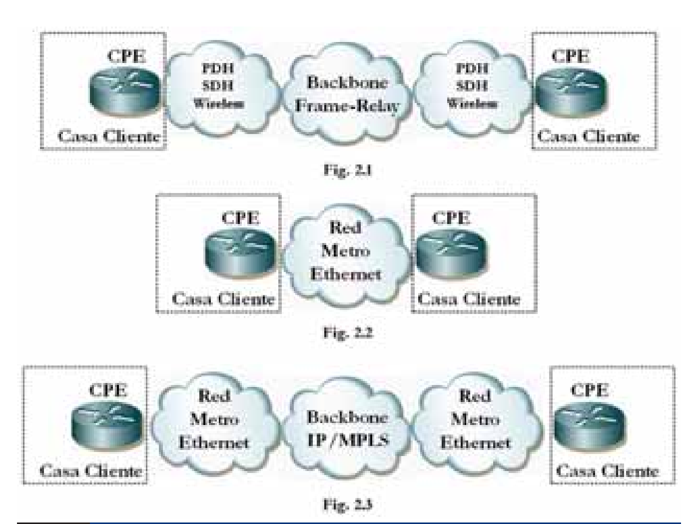


Fig.2 Esquema de los bloques del Carrier

En las redes Metro-Ethernet, una VPN de nivel 2 es implementada con la misma red Metro con lo que la red de Acceso son Switches Ethernet (de distintas jerarquías) interconectados por interfaces GigabitEthernet o TenGigabitEthernet. De esta manera la red de Acceso cumple con los niveles 1 y 2 de la capa OSI. Sin embargo las redes Metro-Ethernet pueden servir de acceso a una Red MPLS para la implementación de una VPN de Nivel 3.

Backbone: como fue explicado anteriormente, el significado de Backbone puede variar dependiendo del tipo de VPN ofrecido por el Carrier, ya que puede ser compuesto por Switches Frame Relay, por Switches Ethernet (para el caso de redes Metro-Ethernet), o por Routers formando un Backbone MPLS.

En la figura 2 se encuentra un diagrama con los bloques descriptos y los tres casos citados que son los más comunes a encontrar entre las redes de los Carriers.

Cada uno de los bloques tienen que tener implementado QoS de manera de poder dar tratamiento especial a cada tipo de tráfico. De esa manera aseguramos que los recaudos que tomamos en el CPE en clasificar el tipo de flujo, darle prioridad y aseguramiento de BW a los tráficos “real time”, serán tenidos en cuenta en los distintos bloques siguientes.

En la figura 2.1 se ve que la red de Acceso (PDH, SDH, Wireless) es determinística, esto es que el BW será reservado para todos los tipos de tráfico que el cliente curse y que en caso de que no sea utilizado, no será utilizado por otro cliente. En la figura 2.2 y 2.3 la red de Acceso es Metro-Ethernet, que por definición es una red de paquetes conmutados. Por lo tanto el Carrier puede optar por sobresuscribir los troncales dándole lugar a la probabilidad de que los clientes no transmitan información durante el 100 por ciento del tiempo. Esto trae como consecuencia que en algún momento se pueda dar el caso de que ciertas troncales puedan congestionarse y hasta incluso llegar al tope máximo de ocupación. En esos casos existen mecanismos para tratar de evitar la congestión y en caso de que esta sea inevitable, tomar medidas sobre los tráficos con menor prioridad.

Estos mecanismos serán explicados en artículos posteriores pero el concepto que debe quedar claro es que así como se le dieron privilegios en el CPE a los flujos “real time” se le pueden y deben dar en el resto de los bloques de la red del Carrier teniendo una consistencia que permitirá brindar una Calidad de Servicio de extremo a extremo. ●

Consistencia en el trato de los flujos

La Calidad de Servicio de extremo a extremo (QoS End-to-end) se logra solamente siendo consistente en la diferenciación y trato de los distintos tipos de tráfico cursados a través de las redes.

Layer 2 Tunneling Protocol v3

Layer 2 Tunneling Protocol versión 3 es la evolución de un conjunto de estándares, que permitían emular circuitos por medio de Pseudowires, con el objetivo de transportar protocolos de nivel 2, tales como Ethernet.

Autor: **Juan Urti**
Ing. en Telecomunicaciones (IUPFA)

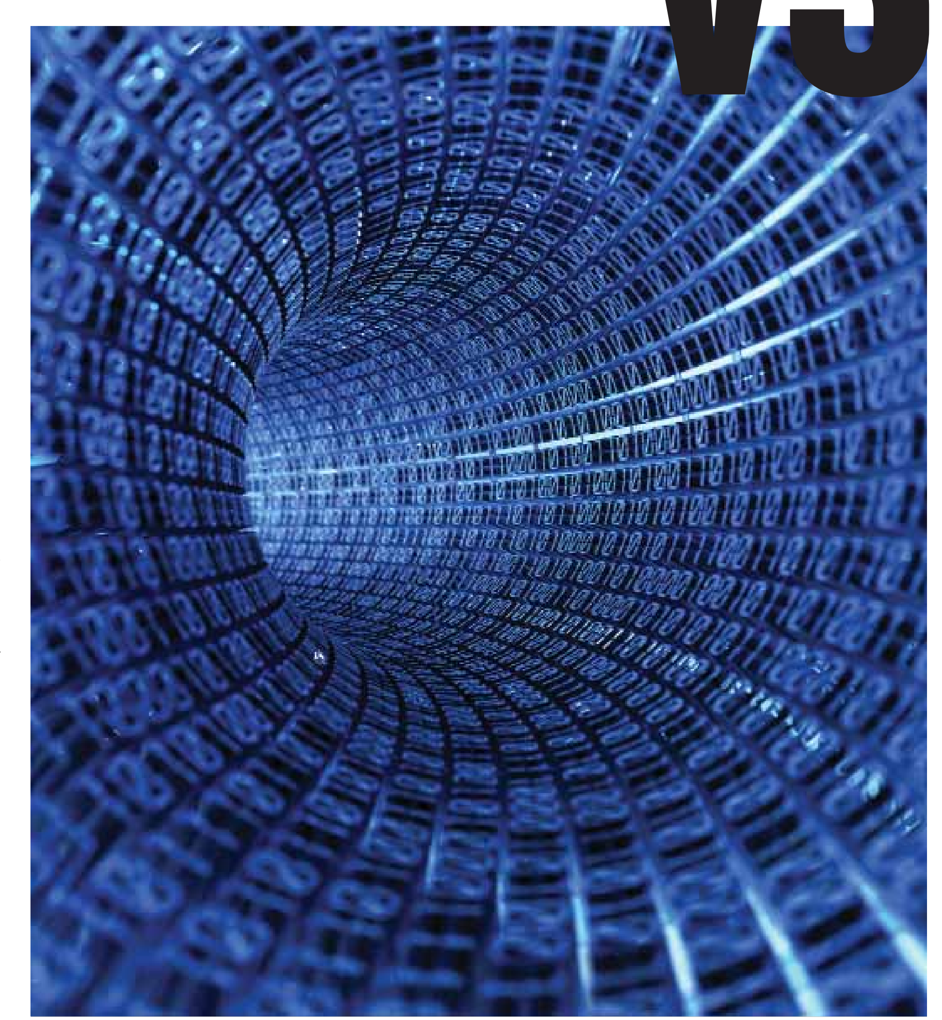


FOTO: (c) istockphoto.com/Andrey Prokhorov

Introducción

El objetivo de esta nota es continuar aquel concepto iniciado en el artículo *"Layer 2 VPN"* en NEX #28, profundizando ahora sí en el protocolo que hace posible tal conectividad, estamos hablando de *Layer 2 Tunneling Protocol versión 3 (L2TPv3).*

L2TPv3 es un protocolo estándar del IETF, el cual permite por medio de Pseudowires (túneles) emular circuitos de nivel 2 en redes basadas en el protocolo IP. Este protocolo a diferencia de sus predecesores, como UTI de Cisco, posee mecanismo de señalización con el objetivo de enviar keepalives para verificar el estado del Pseudowire (PW) o túnel.

No debemos olvidar la principal funcionalidad de este protocolo, que es la de transportar tramas de una capa inferior en tramas de un protocolo superior, exactamente al revés de cómo se acostumbra a realizar. Un ejemplo claro es el transporte de tramas Ethernet sobre un medio MPLS, el cual conceptualmente está arriba en el modelo OSI.

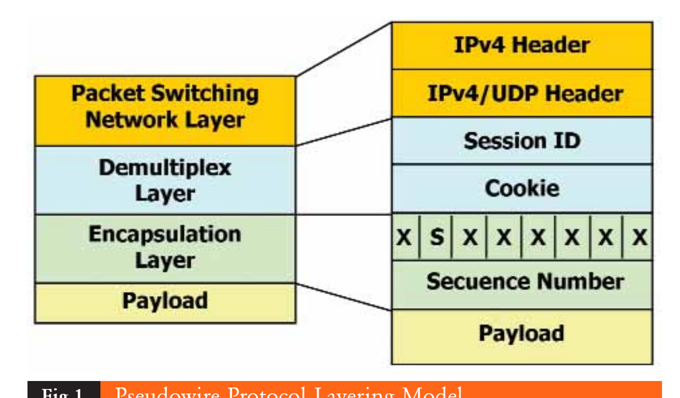


Fig.1 Pseudowire Protocol Layering Model

Arquitectura del L2TPv3

El grupo de trabajo "Pseudowire Emulation Edge to Edge" del IETF, cuyo fin es el de describir los mecanismos mínimos para la encapsulación de datos, desarrolló una arquitectura y un esquema de protocolos con el objetivo de emular circuitos, denominándose tal modelo Pseudowire Protocol Layering Model. A pesar de haberlo ya mostrado en números de la revista anteriores, ahora vamos a verlo en más detalle, como lo observamos en la figura 1.

La capa superior *"Packet Switching Network"* es la encargada de direccionar el tráfico basándose en el paquete IP. Existen dos formas de encapsular los header en esta capa: encapsular solo el header IPv4 de 20 bytes (sin opciones), y sino como alternativa encapsular el header IPv4/UDP que combina ambos encabezados empleando el puerto 1701 (inicialmente para establecer la conexión).

Las ventajas de usar la segunda opción es la facilidad de implementar NAT -Network Address Translation- ya que la encapsulación con UDP tiene en cuenta el port. También es muy útil su aplicación debido a la doble verificación de errores, ya que realizará un checksum con el header IP y con el header UDP para el payload.

La capa *Demultiplexing* permite a un túnel IPv4 (par IP origen destino) transportar y

demultiplexar múltiples PW, permitiendo de esto gracias a las sub capas Session ID y Cookie (esto es muy importante ya que entre dos routers PE puede haber diversos PW con diferentes propósitos).

El campo Session ID posee significado local e identifica una sesión específica entre los dos puntos finales del túnel. Es un sub campo de 4 bytes, reservándose su valor cero para el canal de control (como explicaremos más adelante). El sub campo Cookie puede poseer una extensión nula, de cuatro u ocho bytes y su uso es, previa negociación de una clave por el canal de control, proteger la información de inserciones de datos maliciosos agregados intencionalmente.

Por último, L2TPv3 posee la capa de encapsulación que transporta valores necesarios para la desencapsulación del túnel en el otro extremo, y que no son enviados en el payload. El caso más común de ello son las aplicaciones que precisan de paquetes secuenciados.

Mensajes de Control en L2TPv3

Este protocolo posee un mecanismo flexible, que permite negociar ciertos parámetros luego de la creación del PW. De manera similar a como LDP -Label Distribution Protocol- controla y señaliza los LSP –Label Switched Paths- en MPLS, L2TPv3 también posee su manera simple de realizar la misma labor denotando L2TP Control Connection.

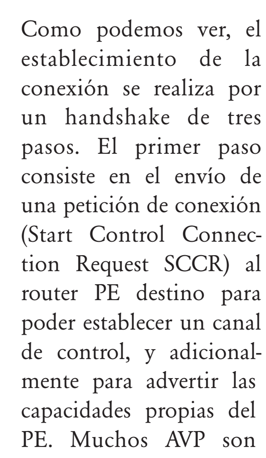
Debido a que estos paquetes de control son enviados *inband* de la conexión, es preciso que exista un método que permita diferenciar los mensajes del canal de control de forma eficiente. Este método consiste en colocar el valor del sub campo Session ID en cero (Mensaje de Control).

Para estas funciones, la capa de Encapsulación se ve modificada en su forma, agregándole tres sub campos llamados "Control Message Header", "Attribute Value Pair" (AVP) y "Additional AVP".

Entre otras posibilidades, con estos campos podemos configurar el número de secuencia de envío del paquete, el número de secuencia de recepción (de manera similar a X.25), el ID de la conexión de control, el vendor ID, el tipo de atributo, etc. Al configurar usted L2TPv3 en algún router PE observará cómo estos y otros parámetros deben ser especificados.

Señalización en L2TPv3

La señalización opera en dos fases: el establecimiento de la conexión L2TP para el flujo de tramas, y el establecimiento de la sesión si fuese necesario. Tomemos como ejemplo a la figura 2.



Como podemos ver, el establecimiento de la conexión se realiza por un handshake de tres pasos. El primer paso consiste en el envío de una petición de conexión (Start Control Connection Request SCCR) al router PE destino para poder establecer un canal de control, y adicionalmente para advertir las capacidades propias del PE. Muchos AVP son enviados aquí, como por ejemplo el Control Connection ID y el Pseudowire Capability List (para la implementación de Layer 2 VPN sobre MPLS). El segundo paso comienza con la respuesta del PE remoto (SCC Replan) enviando al PE origen sus capacidades. Este PE también envía varios AVP. Finalmente, el router que deseo iniciar la conexión envía un tercer paquete denominado SCC Connected, que además sirve como acuse de recibo del SCCRP. Una vez establecida la conexión, ambos PE envían keepalives regulares, con el objeto de chequear la integridad del vínculo, y en caso de por cierto tiempo no recibir ninguno, cerrar el túnel y el canal de control.

Ahora sí creado el vinculo, de manera similar pueden crearse sesiones, las cuales permitirán establecer PW entre los PE (he aquí la importancia del Session ID, ya que entre los routers puede haber PW con diferentes propósitos).

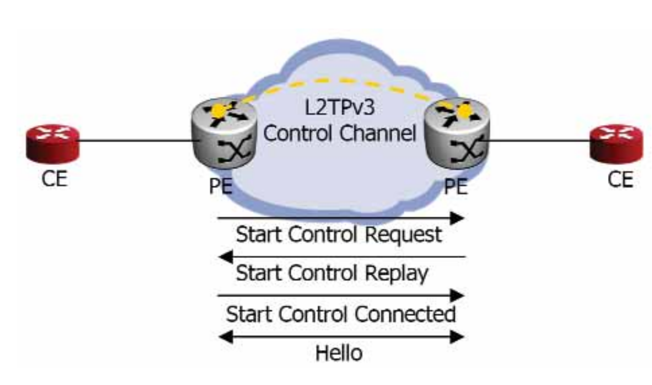


Fig.2 Señalización L2TPv3

Tipos de Pseudowire

Como hemos ya comentado, L2TPv3 es el protocolo que se emplea para emular circuitos de capa de enlace en las redes de nueva generación, o bien como se lo conoce más comúnmente, para crear Redes Privadas Virtuales -VPNs- de nivel dos. No olvidemos que un PW siempre conlleva Any Transport Over MPLS -AToM- y encapsulación L2TPv3.

Este protocolo nos permite crear dos tipos básicos de pseudowires: emulación de circuitos port-to-port; y emulación de circuitos vlan-to-vlan.

El objetivo de este apartado es dejar claro los principales conceptos para en un artículo posterior explicar cómo se encapsulan la gran variedad de protocolos LAN y WAN sobre L2TPv3 y por ende también dentro de los PW.

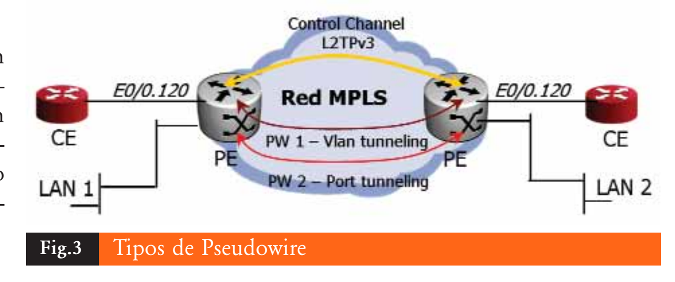


Fig.3 Tipos de Pseudowire

Tomemos la figura 3 para observar los dos casos que hemos mencionado. Se configuraron 2 sesiones dentro del túnel L2TPv3, por lo tanto se crearon dos PW, uno para cada ejemplo (a modo de observación, los túneles por lo general se configuran sobre interfaces Loopback de los PE, ya que estas tratan de ser únicas dentro del dominio MPLS).

Pasemos a explicar el primer caso, el correspondiente al PW 1, el cual vincula dos routers CE (pueden ser Switches de nivel 3) por medio de un dominio MPLS. A pesar de que no haría falta, las interfaces que vinculan los routers con los PE están en modo vlan trunk, y el objetivo nuestro es encapsular la vlan 120, en ambos lados de la figura, sobre el PW. Para tal fin deben crearse subinterfaces en los PE MPLS y dentro de ella declarar qué vlans deseamos que se mapeen en el PW, quedando así solo este tráfico dentro de la sesión (para más detalle, este ejemplo es muy similar al descrito en el artículo "VPNs sobre redes Metro Ethernet" del número anterior, ya que ese vlan ID puede ser el Customer Tag). Por último mencionamos que no es necesario que el vlan ID sea el mismo en ambos extremos, simplemente que para la resolución de problemas es mejor mantener un esquema sencillo y ordenado.

El segundo ejemplo es el denominado port-to-port tunneling, y en él todos los frames Ethernet que llegan al port del PE son introducidos dentro del PW y transportados hasta el otro extremo de la red. Este es el típico caso de un Lan to Lan sobre una red Metro Ethernet/MPLS, en el cual los frames sin vlan ID (o sea los pertenecientes a la vlan nativa), los que poseen IEEE 802.1q y los que llevan doble tag Q-in-Q son replicados transparentemente en el otro PE. ●

Bibliografía

www.cisco.com - Layer 2 VPN Arquitecturas. Cisco Press.2003

Fibra Óptica

Miguel F. Lattanzi
Ing. en Telecomunicaciones (IUPFA)

La importancia de la fibra óptica en las comunicaciones ha sido decisiva, dado que permite transmitir una gran cantidad de información de manera segura y eficaz. En los últimos años han aumentado de forma exponencial los usos de la fibra óptica, utilizándose hoy en día en casi cualquier aplicación tecnología.

Intoducción Histórica

Desde el punto de vista práctico se puede decir que la historia de la fibra óptica comenzó en 1966, cuando Charles Kao en su tesis de doctorado dedujo que el valor de las pérdidas por atenuación de la fibra óptica debía ser igual o menor a 20 dB/Km, para ser utilizada en enlaces de telecomunicaciones.

No fue hasta 1970 que se anunció tal logro, llevado a cabo por Robert Maurer, Donald Keck y Peter Schultz, de la compañía Corning Glass Works (actualmente Corning Inc.), quienes lograron obtener una atenuación de 17 dB/Km para una fibra óptica monomodo. Este avance fue tan determinante que iniciaron un sin número de actividades de investigación e ingeniería relacionadas con la transmisión de la luz en medios guiados.

En el mismo año, investigadores del Instituto de Física Ioffe en Leningrado (actual San Petersburgo), desarrollaron el primer diodo LASER (Light Amplification by Stimulated Emission Radiation) semiconductor capaz de transmitir una onda continua a temperatura ambiente. Durante los años siguientes el valor de las perdidas por atenuación disminuyó casi exponencialmente. Esto se debió, en parte, a las mejoras introducidas en las técnicas de fabricación de la fibra óptica y en el continuo desarrollo de dispositivos que permitieron utilizar mayores longitudes de onda, las cuales son afectadas en menor medida por la atenuación.

Con los avances mencionados, hoy día se han alcanzado índices de atenuación que rondan los 0.5 dB/Km, incluso se han logrado valores menores.

Aspectos Técnicos

Los cables de fibra óptica están constituidos básicamente por el núcleo, conformado por un material con índice de refracción n1; por el revestimiento, el cual tiene un índice de refracción n2 y la cubierta protectora (conocida también como recubrimiento). Para que la luz pueda ser confinada y propagada a lo largo de la fibra óptica se debe cumplir la siguiente condición:

$$n_1 > n_2$$

Decibel (dB)

El decibel –que se indica dB– es una unidad de medida que permite cuantificar la relación existente entre dos valores dados, por lo general uno conocido y el otro variable. En el caso de la fibra óptica se miden los valores de potencia de la señal en ambos extremos de un segmento dado de fibra y se calcula la atenuación reemplazando dichos valores en la fórmula correspondiente. Esta es una característica importante que los fabricantes de fibra colocan en las hojas de datos.




IMANAGING
intel
Core 2
Duo
inside
Dual-core.
Haga más.
Yo, Banghó
Empresario
Hiperconectado
Porque Banghó comprende la idiosincrasia local y aporta soluciones concretas para problemas reales. Porque su innovadora arquitectura tecnológica permite a las empresas enfrentar con éxito operaciones de misión crítica. Porque sus líneas de PCs, servidores y notebooks están certificadas bajo normas de calidad internacionales, brindando mayor poder de procesamiento, almacenamiento, seguridad y conectividad.
Por todo esto, cada vez más argentinos eligen productos Banghó.

Lo cual significa que al índice de refracción del medio 1 debe ser mayor que el correspondiente al medio 2.
En la figura 1 se puede observar un cable de fibra óptica –con los componentes básicos– y la relación que existe entre los medios n1 y n2 en cuanto a la construcción de dichos cables.
El fenómeno de propagación de la luz se da cuando, con los índices de refracción adecuados, la luz se refleja en la superficie de frontera existente entre el núcleo y el revestimiento sucesivamente a través de toda la longitud de la fibra óptica.
Por medio de la ley de Snell –formulada por él mismo en 1621– se puede saber con qué ángulo serán refractadas las distintas componentes de la luz cuando atraviesen la frontera que separa ambos medios, es decir, cuando el haz de luz pasa de un medio de propagación a otro. La ley de Snell establece, por tanto, lo siguiente:

$$n_1 \cdot Sen\theta_1 = n_2 \cdot Sen\theta_2$$

Utilizando esta fórmula se puede obtener el valor de los distintos ángulos, tanto de incidencia como de refracción, o el índice de refracción de los medios de propagación. La ley de Snell se ha transformado en un concepto fundamental para el desarrollo de la óptica geométrica moderna.
Otro factor importante es el ángulo de apertura numérica, el cual define el rango de ángulos incidentes aceptables para el ingreso de los haces de luz al cable de fibra óptica. El mismo esta definido por una relación entre el índice de refracción de ambos medios de propagación.

Tipos de Fibra

Las fibras ópticas pueden ser clasificadas por los materiales de construcción empleados, por los modos de propagación y por las características de los índices de refracción.
Según los materiales utilizados podemos definir dos tipos principales de fibra óptica, las plásticas, conocidas como POF (Plastic Optical Fiber) y las de vidrio, basadas en sílice y dopadas con diversos elementos para mejorar sus propiedades.
Según los modos de propagación se las puede diferenciar en monomodo y multimodo. Las fibras monomodo solo admiten un modo de luz, son utilizadas para aplicaciones que requieren cubrir grandes distancias. Las fibras multimodo son aquellas que pueden propagar varios modos de luz, son utilizadas en aplicaciones de corta distancia y son más fáciles de fabricar –y por ende más económicas– que las monomodo.
En cuanto a los índices de refracción, se las puede dividir en índice escalonado (o salto de índice) e índice gradual. Las de salto de índice tienen un índice de refracción constante en toda la sección circular del núcleo. Las de índice gradual, por el contrario, tienen un índice de refracción que disminuye conforme aumenta la distancia desde el centro de la sección circular del núcleo.

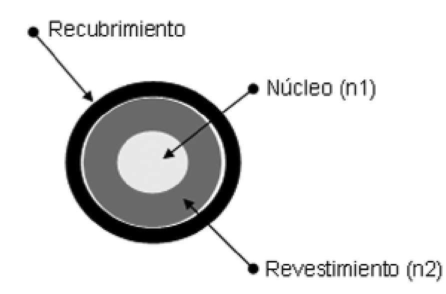


Fig. 1 Modelo básico de un Cable de Fibra Óptica

Aplicaciones

Los campos de aplicación de la fibra óptica son cada vez mayores, abarcando desde la transmisión de datos en redes de telecomunicaciones hasta propósitos decorativos, sin embargo, el mayor impacto se produjo en el campo de las comunicaciones.
Gracias a la evolución de los cables de fibra óptica fue posible obtener redes de telecomunicaciones con grandes capacidades de transmisión de datos, las cuales son utilizadas extensivamente. Los fabricantes de equipos de comunicaciones se han adaptado para poder aprovechar al máximo las cualidades de la fibra óptica, con ello los prestadores de servicios –quienes son los compradores de dichos equipos– han definido nuevos tipos de servicios a ofrecer para los usuarios y las empresas demandantes del mercado. Las grandes ciudades del mundo tienen gran cantidad de fibra óptica instalada para interconectar los nodos de comunicaciones principales. Existen, asimismo, una gran cantidad de cables submarinos que unen los distintos puntos de los continentes e incluso cruzan los océanos para interconectar a los continentes entre sí. Entre las aplicaciones más comunes y más importantes, a parte del campo de las telecomunicaciones, podemos destacar las siguientes:
Aplicaciones Médicas, son utilizadas con dispositivos LASER para llevar a cabo cirugías. También se las utiliza para realizar endoscopias.
Aplicaciones Arqueológicas, son utilizadas para poder observar el interior de lugares muy estrechos, como ser el caso de grietas y fisuras.
Aplicaciones Industriales, se las utiliza como lentes de observación para poder inspeccionar el interior de los objetos a través de orificios pequeños. Pueden inspeccionarse electos tan variados como ser turbinas de aviones o el interior de tanques que soportan altas presiones.
Sistemas Autónomos, empleadas para el procesamiento de datos y comunicaciones en entornos reducidos como ser el caso de los aviones, ya sean militares o civiles.
Usos Decorativos, se utilizan para iluminar maquetas, decorar árboles de navidad, en la construcción de dispositivos decorativos para los hogares e incluso para la iluminación de cuadros. Cabe aclarar que éstas son solo algunas de las aplicaciones que hoy en día hacen uso de los beneficios de la fibra óptica, el número de aplicaciones ha ido en aumento, a una velocidad sin precedente, en los últimos años.

Ventajas y Desventajas

Entre las ventajas inherentes al uso de la fibra óptica para aplicaciones de telecomunicaciones podemos mencionar:

- Gran capacidad de transmisión de datos.
- Baja atenuación.
- Baja tasa de errores de datos.
- Inmune ante interferencias electromagnéticas.
- Seguridad física elevada, es difícil interceptar los datos.
- Abundancia de los materiales que las constituyen.

Como desventajas podemos enumerar a las siguientes:

- Equipos de comunicaciones caros.
- No se puede transmitir electricidad para los repetidores.
- Fragilidad de los pelos de fibra.
- Dificultad a la hora de realizar reparaciones.

Esta claro que el mercado cada vez demandará con mayor fuerza la instalación de cables de fibra óptica, en función de la demanda de ancho de banda que cada año va en aumento. Aún hoy los costos de instalación de fibra no son baratos, y los proveedores de servicios tienen una planta externa –a lo que la primera milla se refiere– casi enteramente conformada por enlaces de cobre, y en menor medida de radio.
Por otro lado, los nuevos servicios de datos basados en tecnologías xDSL permiten continuar aprovechando la gran cantidad de pares de cobre ya instalados con velocidades de transmisión de datos y ancho de banda elevados.
Todo esto contribuye a demorar la decisión de instalar, en forma masiva, fibra óptica en la red de acceso. Sin embargo, nuevas tecnologías como GPON (Gigabit Passive Optical Network), BPON (Broadband Passive Optical Network) y EPON (Ethernet Passive Optical Network), están acercando la fibra hasta los límites del abonado.
Con estas nuevas tecnologías, poco a poco, el uso de la fibra óptica como medio de transmisión en las redes de acceso se hará más extensivo y los costos de instalación irán disminuyendo conforme se masifique esta práctica. ●

Triple Play

El camino hacia la unificación de los medios

Esta tecnología es el futuro cercano para el desarrollo integral de servicios de telecomunicaciones hogareñas y empresariales.

Ing. Marisabel Rodríguez
Networking Supervisor

Qué brillante idea la de convertir en datos lo que hablamos por teléfono, lo que vemos por televisión y transmitirlo por un mismo canal, bi-direccional, redundante, con escalabilidad y seguro, junto con el tráfico de banda ancha.
No estamos muy lejos de que este servicio sea algo cotidiano, realmente estamos en un estado del arte en la tecnología, que permitirá que en pocos años sea masivo. En Estados Unidos, la empresa de Telecomunicaciones SureWest (www.surewest.com) ya vende servicios Triple Play, y no tardará mucho en tener competidores fuertes en el mercado.
Triple Play se define como el empaquetamiento de servicios y contenidos audiovisuales como voz, banda ancha y televisión. El servicio Triple Play es el futuro cercano para el desarrollo integral de comunicación en los hogares. El desarrollo actual de los ISP conlleva una solución única para varios problemas. El servicio telefónico, televisión interactiva y acceso a Internet, todo se transmite en un mismo medio físico basado en ADSL. Así se posibilita un servicio más personalizado debido a que el cliente dispone de las prestaciones y contenidos que el desea utilizar en el momento que realmente quiere. Otro beneficio importante es que se mejora la calidad de los servicios, llevando hasta los hogares la calidad digital en televisión, sin olvidar las nuevas posibilidades en telefonía y un abaratamiento del acceso a Internet.
Por eso cada vez más compañías telefónicas que ofrecen servicios de conectividad a Internet están promocionando servicios de voz, datos y video a los clientes. El hecho de que una empresa brinde buenos servicios en un mismo paquete incrementa la lealtad de los clientes y fortalece la presencia en el mercado de sus productos.

TV sobre IP

La televisión sobre IP está ganando un gran impulso, las compañías telefónicas están viendo un nuevo horizonte y muchas oportunidades de negocio. Los servicios Triple Play utilizan tecnología de ADSL, VDSL, fibra, LMDS, Wireles Lans y WiMax.
La idea sería transmitir sobre redes IP los servicios usuales de TV, TV interactiva y TV en las computadoras personales. Esta última aplicación es una de las características más sobresalientes que marcan la versatilidad del sistema: los usuarios pueden ver televisión tanto en sus televisores como en sus computadoras. Las compañías telefónicas y los operadores de cable, en determinado momento, tenderán a utilizar esta tecnología ya que la desregulación incrementó la competencia en los mercados telefónicos tradicionales y deberán abrirse camino en el nuevo paradigma. El advenimiento de este nuevo servicio les abre la posibilidad de incrementar sus ganancias y la porción de mercado que poseen. El hecho de que los clientes reciban los servicios desde una misma interfaz, de un solo proveedor resulta más fácil de mantener, más fácil de facturar y se puede llegar a mejorar muchísimo el servicio al cliente unificando el soporte. Además, utilizando redes digitales, las compañías telefónicas y los operadores pueden ofrecer paquetes comerciales más sofisticados.
Con TV sobre IP pueden transmitirse entre 50 y 200 canales. El contenido se transporta en un stream desde el Head-End (Oficina Central) del operador, a través del Backbone, hasta un Nodo Regional.
En el Nodo Regional el video se distribuye en la última milla hasta el usuario final. Además, el equipo de streaming en la Oficina Central permite a los operadores insertar canales adicionales de contenido local que pueden ser enviados a áreas específicas o grupos de usuarios. Mientras que la estructura de la red puede diferir, para el consumidor final el método de distribución es transparente.

La televisión sobre IP está ganando un gran impulso, las compañías telefónicas están viendo un nuevo horizonte y muchas oportunidades de negocio.

¿Qué se necesita para implementar este cambio?

Además de una la infraestructura de red importante y de gran ancho de banda para poder hacer streaming de video y voz, se necesitan equipos en el Head-End, en los Nodos Regionales y en el lugar donde se encuentran los clientes.
La plataforma de streaming reside en el Head-End (u Oficina Central), donde se reciben los streams analógicos y se digitalizan. Luego se transmiten los datos hacia un switch o router, que los envía luego por el Backbone a los Nodos Regionales remotos, y desde allí, al consumidor. También puede haber una plataforma adicional de streaming en la Oficina Central, que puede distribuir transmisiones locales, y mandarlas a determinadas áreas.
La plataforma de streaming debe cumplir ciertos requisitos. Primero, necesita poder transferir datos digitalizados con alta calidad, debe poder transportar la información con el bit-rate que proviene de por ejemplo un satélite, y luego pasarlo a un ancho de banda de 2 a 4 MB para la infraestructura DSL. Como el video se está distribuyendo en una plataforma de telecomunicaciones, la arquitectura debe cumplir con los standards de Carriers, con

gran ancho de banda, redundancia y capacidad de recuperación ante fallas.
Los Video-Servers, tienen varios propósitos en los Head-Ends. Se utilizan para guardar y retransmitir información, guardan contenidos digitalizados y los convierten en un stream de datos que envían a equipos pertenecientes a la infraestructura de red. El propósito principal es recibir y enviar los contenidos que se codifican digitalmente de las plataformas de Play-Out. La forma de operar es codificar todos los canales diariamente, subiendo los contenidos a un Video-Servidor. Los espectadores, desde sus casas podrían ver cualquier programa cuando quieran, siempre dentro de los que están disponibles con el paquete que han comprado.
Los dispositivos de ruteo de redes, transportan la transmisión de datos por Multicast. Los routers o switches que están en la Oficina Central hacen de interfaz con toda la red. Reciben los datos y transmiten a otros DSLAMS ubicados ahí, o sino hacia la red ethernet del usuario.
El DSLAM (Digital Subscriber Line Access Multiplexer), reside en la Oficina Central, conecta a los usuarios de ADSL (o más bien xDSL) al Backbone y al Head-End. Cuando se distribuye TV sobre IP, el DSLAM debe soportar el método de Multicast, sino el equipo de la Oficina Central debería replicar cada canal para cada pedido de los usuarios, lo que puede ocasionar cuellos de botella en el DSLAM.

El esquema de una Red IP con Multicast puede lograr que una sola copia de la información de cada canal llegue a los switches de distribución, y de ahí se mande solo a los usuarios que quieren verlos.

CPE (Customer Premises Equipment), es usualmente el modem DSL, se encuentra del lado del cliente, y recibe el stream de TV sobre IP. El módem DSL recibe el stream del DSLAM o sino de un equipo capa 3 y lo transfiere directamente a la PC para mostrarlo en el desktop o en el IP STB (IP Set Top Box). Este equipo recibe el stream IP, lo decodifica y lo muestra. Por lo general, el STB recibe el stream del CPE. Algunos STBs pueden recibir el stream directamente del DSLAM, y sirven como CPE también.
La configuración del equipo final está alojada en el CPE (Customer Premises Equipment), en la mayoría de los casos es un módem, que transfiere streams de MPEG-2 o MPEG-4 hacia un IP/STB que decodifica los datos que le llegan para que luego se vean en el televisor. Los streams de MPEG-4 se pueden ver también en la PC usando el Microsoft Media Player. Si hay ancho de banda suficiente entre la oficina central y el punto en donde se encuentra el cliente, se pueden mostrar varios canales al mismo tiempo.



Otra de las formas posibles de implementación, para citar otro esquema, es a través de una solución que se está utilizando con éxito en los Estados Unidos, que requiere una comunicación FTTH (Fiber To The Home) del lado de los usuarios. Aunque no necesariamente se necesita FTTH, porque el requisito es de solamente 20M para HDTV, voz y datos.
La empresa SureWest está ofreciendo de esta forma 275 canales de video y audio Standard y 17 canales de alta definición, además de alrededor de 900 horas de programación de Video On Demand.
Esta modalidad de distribuir los servicios es una gran ventaja para la empresa, ya que se simplifica la entrega de datos, voz y video, y facilita el monitoreo y la evaluación de la performance de la red.
El hecho de que se llegue hasta los usuarios con video a través de una red, permite que se puedan utilizar las características del tráfico Multicast, aprovechando al máximo el ancho de banda. La estructura de una red que provea estos servicios debe contar con switches de Core muy potentes, y otros de Distribución con alta densidad de bocas y alta velocidad para poder llegar con el mayor ancho de banda posible a los usuarios finales.
Dentro del equipamiento también se necesitan receptores satelitales para obtener las señales a transmitir, y servidores de VoD (Video on Demand), además de equipos de VoIP y de datos.
De esta manera, los switches con bocas de fibra, llevan 100M de información hasta los hubs donde se distribuye luego el tráfico hasta los clientes. Por ejemplo, un Switch de Core, puede abastecer a 40000 clientes, ayudado por los switches de Distribución, y los hubs. Con esta configuración se puede aplicar QoS (Quality of Service), y las capacidades de Multicast para transmitir IPTV y HDTV.
Mientras que las infraestructuras de los Operadores de Cable tradicionales distribuyen el cable en las casas de los usuarios uno a uno, el esquema de una Red IP, puede lograr que una sola copia de la información de cada canal llegue a los switches de Distribución, y de ahí se mande solo a los usuarios que quieren verlos. En cada punto de la red, hay una sola copia de cada canal. De esta forma se ahorra muchísimo ancho de banda con respecto a otro tipo de arquitecturas que transportan múltiples copias, a pesar de que ninguno en el barrio quiera ver algunos canales. La clave es usar las capacidades del protocolo IGMP (Internet Group Management Protocol) para distribución de video. Es una forma mucho más inteligente de broadcast. Además se puede agregar todo tipo de restricciones y evitar, por ejemplo, que ciertos usuarios que ya estén viendo un programa, puedan tener un menor ancho de banda al agregarse más clientes que quieran ver lo mismo, y así requieran más recursos de los que fueron dimensionados.

Los servicios de video streaming son un ingrediente fundamental de la receta Triple Play para crear nuevas fuentes de ingreso y lealtad del cliente.

En una red NGN (Next Generation Networking) como la que describo, los equipos de red pueden tener la suficiente inteligencia como para replicar un determinado canal según sea necesario, y llevarlo solamente al hogar que lo está pidiendo. Como la información se envía solamente a los lugares en donde se precisa, se gana mucho ancho de banda, dependiendo del diseño de la red.

Muy pronto estaremos disfrutando de los más variados servicios de video, telefonía y datos. Ya existe la tecnología, solo depende de la creatividad de las empresas y las reglas del mercado en el país. Pero esa es otra discusión. ●

Sun Tzu y la Telefonía IP

Autor: **Cristian Venegas**
Systems Engineer **- Cisco**

Conozca la infraestructura y las aplicaciones necesarias para lograr la seguridad en la Telefonía IP.

Internet se ha convertido en un campo de batalla. El hacking dejó de ser una actividad exclusivamente académica, conducido por un reducido grupo de elite, ávidos de conocimiento, altamente capaces y motivados por la curiosidad. Hoy en día, el escenario es otro: existe una impresionante cantidad de herramientas disponibles al alcance de cualquier persona con acceso a Internet, y una importante tendencia que describe la principal motivación del hacking con un foco económico. Tecnicismos como el phishing, zombies, bot-nets, grayware, spear-phishing, spamming, fuzzing, sniffing, DoS, SPIT, entre otros se hacen cada vez más familiares. Viejas técnicas, pero igualmente efectivas, como la ingeniería social siguen siendo practicadas para alcanzar la meta.

Uno de los más importantes párrafos del libro "El Arte de la Guerra" (de Sun Tzu), dice así: "Conoce a tu enemigo y conócete a ti mismo; en cien batallas, nunca saldrás derrotado. Si eres ignorante de tu enemigo pero te conoces a ti mismo, tus oportunidades de ganar o perder son las mismas. Si eres ignorante de tu enemigo y de ti mismo, puedes estar seguro de ser derrotado en cada batalla".
Efectuando un barrido rápido por lo que fue una de las convenciones de hackers más importantes del año pasado -BlackHat 2006 realizada en las Vegas- y una revisión del contenido de las presentaciones allí encontradas,



revela un foco en voz sobre IP y telefonía IP sobre estos temas:
- Utilización de herramientas como Google y Nmap para el reconocimiento de vulnerabilidades sobre sistemas de telefonía IP.

- El uso de software como Sivus, Netscan y SIPScan para generar ataques de negación de servicio, en la que el normal funcionamiento de una plataforma de telefonía IP podría estar comprometida.

- Captura de tráfico de la red, tanto como la señalización (el lenguaje utilizado por la infraestructura de telefonía IP para término y establecimiento de llamadas), como el audio transportado sobre una red IP, usando herramientas como Ettercap, Dsniff, Cain & Abel, VoMIT, VoIPong, entre otros.

- El desarrollo de herramientas para generar llamadas telefónicas indeseadas sobre IP, o bien SPIT (Spam Over Internet Telephony).

- Ataques contra carriers IP, que transportan millones de minutos de tráfico de llamadas internacionales originado desde redes de telefonía tradicionales y telefonía IP.

- Utilización de ingeniería social como arma de VoIP phishing, o bien fraudes de distinta índole basado en la interacción persona-persona. Lamentablemente, al día de hoy, no existe un parche para el "descuido" humano.

Antes de describir un posible acercamiento frente a la problemática de seguridad y telefonía IP es necesario tomar distancia un momento, y efectuar un importante análisis. La telefonía IP es transportada sobre una red de datos. Existe una amplia gama de aplicaciones sobre una red de datos, como por ejemplo bases de datos, aplicaciones de facturación, ventas, tráfico web, e-mail, entre otros. En esta lista ¿dónde se posiciona la voz? La pregunta se fundamenta en un tema no menor: en la medida que se incrementan los niveles de seguridad se pueden incrementar los costos. Algunos de estos costos son:

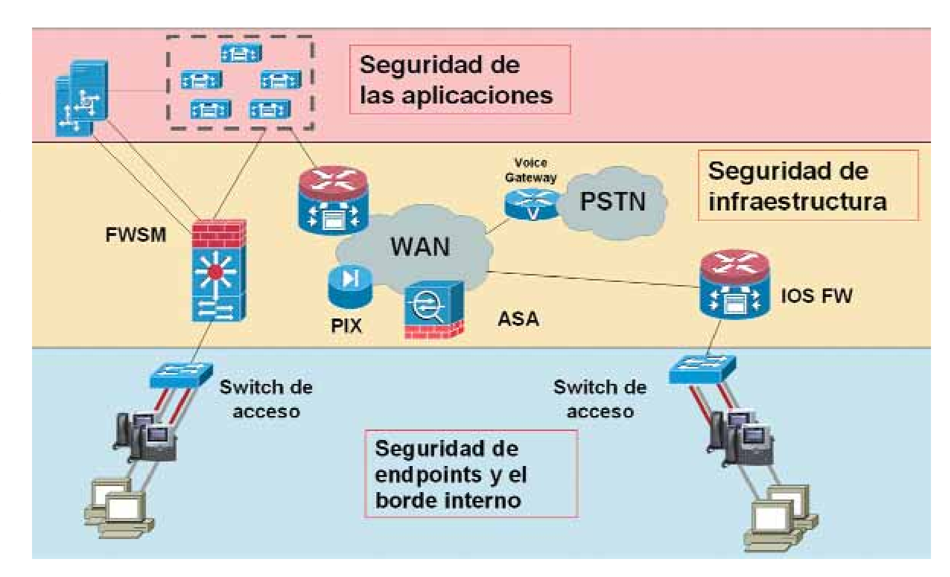
- Áreas de TI necesitan mayores habilidades.

- Puede resultar en up grades a la red o en nuevos equipos.

- Puede afectar la experiencia del usuario final.

- La administración y el troubleshooting pueden ser más complicados, se traduce en tiempo fuera de servicio.

En el contexto de seguridad y telefonía IP, si



pensamos en un automóvil de los años 50 con una serie de enormes almohadones amarrados a sus costados, y a su lado un moderno vehículo, la principal diferencia reside en que la seguridad es un agregado en el primer automóvil, mientras que en el segundo fue algo que se pensó desde el día en que fue diseñado: frenos ABS, airbags, chasis deformable, barras laterales, entre otros son parte integral de la arquitectura del vehículo. De la misma forma se debe manejar la seguridad en la red: no como un adicional, sino como una necesidad que debe estar incluida desde el día que se diseña. La seguridad debe ser tratada como un tema completo, oolítico, de principio a fin y que abarca a todos los elementos de la red: usuarios, endpoints, servidores, switches, routers, etc.
Un acercamiento frente a la problemática de seguridad y telefonía IP puede basarse en un enfoque identificando las principales capas que la componen. Es decir: los teléfonos y del borde interno de la red, la infraestructura, y las aplicaciones y servidores de telefonía IP. Cada una de estas capas tiene propiedades sumamente particulares que revisaremos en mayor profundidad, intentando alinear esta metodología con los ataques en boga que hemos descrito anteriormente.

Seguridad de Endpoints y borde interno

La posibilidad de que la plataforma de administración de los teléfonos IP sea comprometida, o bien exista un ataque del tipo man-in-the-middle, puede ser mitigada usando firmware firmado y archivos de configuración firmados. Esto previene la corrupción de ambos archivos que son claves para la operación.
Desde una perspectiva física, y considerando que se trate de teléfonos con puertos que permitan conectar a un PC atrás del mismo, pueden haber ciertos escenarios en los que no sea necesario, por ejemplo un teléfono IP en un lobby, de acceso público. También puede ser válido deshabilitar la posibilidad de que el usuario final configure el teléfono IP a través de un botón de configuración, así como acceso web, dado que el acceso remoto a los datos específicos de configuración de un teléfono IP constituyen una poderosa herramienta de reconocimiento remoto: direcciones IP, subredes, router por defecto, servidores DNS, servidores DHCP, servidores de configuración, entre otros. Sin embargo, deshabilitar el acceso remoto a la configuración web de un teléfono IP puede tener consecuencias inesperadas que deben ser evaluadas.
Se recomienda también el uso de direccionamiento privado (RFC 1918), así como la separación del tráfico de voz y datos usando VLANs distintas, a pesar que la brecha se está haciendo cada vez más fina (por ejemplo Softphones).
Un tema interesante constituye el tráfico que los teléfonos IP reciben y envían, tanto entre si como a servidores externos. Específicamente, se puede esperar que exista tráfico de señalización, asignación de direcciones IP (ej.: DHCP), configuración (ej.: TFTP), y audio (ej.: RTP). Prevenir el envío de otro tipo de tráfico inesperado a los IP phones puede disminuir en gran medida ataques de negación de servicio.
El tráfico de señalización, es decir aquel que permite establecer y terminar llamadas, así como efectuar servicios complementarios, también debe contar con un buen nivel de seguridad. Para este caso se puede pensar en transportar el tráfico de forma segura. Un ejemplo puede ser usando TLS – Transport Layer Security – RFC 2246 y SIP. Lo mismo es válido para el audio, por lo que un teléfono IP con soporte para audio encriptado (sRTP – Secure RTP) agrega valor a la solución. De esta forma, aunque un atacante pueda efectivamente capturar trafico, se le hará bastante





VXL es reconocida como la mejor opción en cliente delgado en cuanto a precio y beneficio. Con sus nuevos modelos VXL ahora ofrece el rango más amplio en la Industria. Junto con su garantía de tres años y una cadena de soporte a nivel mundial puede comprar los productos ***VXL*** ¡con confianza!

La Solución Thin-Client de Mayor Costo-Beneficio



Itona "Diseñado para Citrix":

- Serie Itona TC45xx & TC 46xx inalámbrico
- Suite de clientes instalado para los productos Citrix
- Funcionalidad completa para el usuario de Citrix al precio más bajo
- Procesador de 1Ghz VIA C7 el chipset más avanzado en la industria
- Opción de Linux, Windows CE o XPe
- Rebate instantáneo de US$20 para usuarios Citrix



Desktop Integrado Itona:

- La nueva solución integrada TI54xx
- Pantalla de 17" LCD
- LAN inalámbrico interno & 10/100 Ethernet
- Opción de Linux, Windows CE o Xpe
- La opción integrada de mejor precio en el mercado



Cliente Delgado Itona Laptop:

- La nueva serie en formato laptop TL37xx
- LAN inalámbrico interno
- Puerto PCMCIA para tarjeta celular opcional
- Opción de Linux o Windows Xpe
- El verdadero cliente delgado móvil

Algo más: Todos los equipos VXL incluyen la licencia de XLmanage, el poderoso software de administración remota y son respaldados por medio de nuestra infraestructura global de soporte incluyendo el servicio de personalización de configuración para proyectos especiales.

Para mayor información contáctese con:



Distribuidor Mayorista Regional de Valor Agregado
Chile: +562/446-8462 | **Brasil:** +5511/6847-4984
Argentina: +5411/4328-3939
vxl@globalsoftware.com.ar



Itona el Cliente Delgado Desktop Líder del Mercado

- Sistemas Operativos Linux, MS Windows CE y Xpe
- Totalmente silencioso, diseño sin ventilador y sin partes con movimiento
- Gráfica de 32 bits capaz de resolución hasta 1600 x 1200
- Gráficas integradas "trident blade 3D"
- Opción de 10/100 Ethernet y adaptadores de LAN inalámbricos
- Lector de "Smart Card" opcional
- 4 x Puertos USB 2.0, serial, paralelo y audio
- Emulaciones incluyen Citrix ICA, RDP, VNC & Unix/IBM

difícil intentar descifrar audio y datos de la llamada. Nuevamente, habilitar estas características puede tener efectos colaterales que deben ser evaluados. Un ejemplo puede ser que un firewall pierda la capacidad de decidir qué puertos de audio abrir o cerrar, puesto que la señalización ya no es visible (¡ahora está encriptada!), por lo que se hará necesario abrir un rango de puertos predeterminados, lo cual puede ser considerado por mucha gente como una vulnerabilidad en sí. La tecnología crea soluciones a sus propios problemas, dice un conocido dicho.

Un poco más adelante en la red se encontrará un switch de acceso. Un servidor DHCP no autorizado conectado al switch puede provocar ataques de negación de servicio, asignando direcciones IP y otros datos claves para la conectividad de los PCs y teléfonos IPs no autorizados. Un switch con algún mecanismo de litigación de este escenario, conocido como DHCP snooping, puede reducir en gran medida este riesgo. El mecanismo puede tener de forma explícita control sobre qué puertas se pueden esperar respuestas DHCP, y ofrecer mitigación filtrando el tráfico, o bien bajando una puerta del switch desde la cual se generan estas respuestas DHCP no autorizadas.

Otro típico ataque, conocido como man-in-the-middle (que es factible de efectuar usando las herramientas mencionadas anteriormente), consiste en un abuso del protocolo ARP, encargado de efectuar la asociación entre direcciones de capa 2 e IP. Parte del protocolo incluye GARP (Gratuitous ARP), es decir el "auto-anuncio" no solicitado por parte de un host hacia la red diciendo "aquí estoy, mi dirección IP es X y mi MAC es Y". Esto puede ser usado para engañar a un host haciéndole creer que un atacante es en realidad un router, y por otro lado, haciéndole creer a un router que el atacante es un teléfono IP. Como consecuencia, todo el tráfico pasa a través del atacante: ni el router, ni el teléfono IP se enterarán que su tráfico está siendo capturado o alterado. Un switch con una funcionalidad de inspección de ARP puede efectuar asociaciones entre una puerta específica y un host específico, de forma dinámica. ARP no incluye el concepto de puerta física de switch, por lo que el ataque es mitigado.

Un símil de este ataque puede ocurrir en la capa superior, es decir en IP, pero si el switch cuenta con algún mecanismo, se puede mitigar un ataque en el que un atacante que intenta hacerle creer a un host atacado que está recibiendo trafico desde cierta IP cuando no es así (termino técnico = IP spoofing).

Para terminar con este punto es importante destacar que se vislumbran en el futuro importantes mejoras con la introducción de 802.3ae, o bien Link Layer integrity, que ofrecerá servicios de confidencialidad en redes alámbricas y que actualmente se encuentra en su quinto borrador en el IEEE.

Seguridad de infraestructura

Toda la infraestructura dentro de la red, llámese equipos de core, distribución, bloques de switches, WAN, e interconexión a la red pública telefonía (PSTN) también debe contar con un nivel de seguridad consistente. Dado que el tema seguridad de infraestructura ha sido abordado en incontables ocasiones, y que el foco de este artículo es sin duda la telefonía IP, será desarrollado con esa óptica.

Los gateways, aquellos equipos encargados de conectar el mundo de conmutación de circuitos con el mundo IP, traducir de forma transparente la señalización de un lado a otro, paquetizar y comprimir la voz, entre otras funciones, constituye un punto interesante. Aquellos gateways que no contasen con un nivel de seguridad apropiados, podrían ser vulnerados para generar, por ejemplo, fraudes telefónicos de llamadas locales, nacionales o internacionales. Es por esto que se puede pensar en un esquema en el que la señalización sea transportada sobre un túnel IPSec, ofreciendo así autenticación, integridad y confidencialidad de este trafico. Adicionalmente, encriptar el audio usando sRTP es altamente recomendado, pero, nuevamente, se deben analizar cuáles son las consecuencias de así hacerlo. En networking, tal como en la economía, se encuentra uno a menudo con la cruel ley de costo-beneficio.

No está de más, y de forma muy breve, recomendar buenas prácticas en la red como por ejemplo:

- Administración usando protocolos que implementen encriptación (ej.: SSH, SNMP v3, HTTPS) o bien intentar usar túneles IPSec cuando esto no sea posible (ej.: para el uso inamovible de telnet).
- Tener una política de logging centralizado y con verificación de su integridad (ej.: vía CRC).
- Respaldos de configuraciones para casos de emergencia.
- Proteger protocolos de enrutamiento con autenticación.
- Implementar sistemas de prevención de intrusos en la red.
- Manejar el ancho de banda para ciertos protocolos típicamente abusados (ej.: ICMP y otros).
- Implementar listas de acceso.
- Contar con una política de administración de seguridad.
- Utilización de host-IPS protegiendo contra amenazas de día cero.
- Sacarle provecho a todas las ventajas de los features de seguridad presentes en los switches: Dynamic ARP inspección, Source Guard, DHCP snooping, BPDU-Guard, port security, VACLS, y muchos más.
- Efectuar scanning de vulnerabilidades, servicios de ethical hacking y consultoría para verificar en qué estado se encuentra la red.
- Verificar el tema de los sistemas operativos, contar con una política de patch-management

Seguridad de las aplicaciones

Si la plataforma de administración de telefonía IP de una empresa llegara a estar comprometida, podría llegar a ser bastante complejo. Desde ataques de negación de servicio, fraude telefónico, compromiso de confidencialidad y sus consecuencias (monetarias, mala publicidad, etc.), son un escenario bastante nefasto, por lo que se hace necesario contar con una política





para minimizar el riesgo.
A primera vista, un firewall suena como una opción bastante plausible. Por cierto, debe ser uno que funcione en modalidad stateful, que sea capaz de comprender protocolos simples y complejos, y seguir de principio a fin una conversación que puede componerse por el uso de puertos (TCP/UDP) fijos y efímeros (aquellos que son utilizados de forma dinámica y por un breve período de tiempo). Si un firewall no es capaz de comprender e inspeccionar protocolos de señalización como SIP, H.323, MGCP o SCCP, entonces no quedará más opción que abrir un rango de puertos para permitir el paso del trafico (ej.: audio/RTP), lo cual no es para nada recomendable. Nuevamente, limitar el ancho de banda de ciertos protocolos también puede ser interesante. Típicamente no se van a esperar cientos de megabits por segundo de tráfico de señalización (que me perdonen aquellos gigantescos proveedores de servicio allá afuera). El mismo firewall debe estar dimensionado para manejar prioridad del tráfico de voz por sobre otros tipos de tráfico. En escenarios de telefonía IP, no se recomienda llegar a umbrales que superen el 60 por ciento de utilización de CPU de los firewalls que estén transportando tráfico de telefonía IP, dado que podría comprometerse la calidad del servicio telefónico. El dimensionamiento para cubrir necesidades actuales, así como las de crecimiento al mediano plazo debe ser considerado al momento de tomar una determinación por un firewall. También se recomienda contar con redundancia ante casos catastróficos (y otros no tanto).
Entrando en campos más escabrosos, la inspección de tráfico de señalización de telefonía IP puede prevenir muchos ataques como DoS, buffer overflows, abuso de protocolos, limitar tráfico indeseado (ej.: desde y hacia ciertos dominios, números y usuarios), uso de recursos no autorizados (ej.: mensajería instantánea sobre SIP), o bien prevenir el paso de tráfico que no sea RTP a través de los media pinholes (puertos que han sido autorizados por el firewall previa señalización), entre otros. Implementar listas negras también puede ser una opción.
Muy a menudo las aplicaciones de telefonía IP están montadas sobre sistemas operativos sumamente conocidos. Si se habla de un modelo appliance, adorado y temido por muchos, de igual forma existe la probabilidad de abuso de vulnerabilidades. Para minimizar este riesgo se puede implementar un Host IPS en la máquina de forma tal que no limite el desempeño normal de las aplicaciones, pero que sí prevenga contra ataques y comportamientos anómalos. Por ejemplo, si se sabe que solo ciertos procesos con nombre y apellido tienen permiso para levantar puertos TCP conocidos, al momento que ocurra alguna anomalía, esta acción puede ser cancelada y reportada a un administrador. Lo mismo puede hacerse en el momento que una interfaz de red pasa a modo promiscuo, lo cual significa que existe algún proceso que se encuentra capturando trafico (sniffing). Tomar acciones automáticas, registrar este comportamiento y reportarlo puede ahorrar muchos dolores de cabeza.
Se recomienda también el acceso a la plataforma de configuración y de gestión de telefonía IP a través de un canal seguro, usando HTTPS por ejemplo. Un timer de inactividad también es un deseable, así como un botón de logoff, la capacidad de definir múltiples perfiles y el registro y sistema de reportaría correspondientes.
El fraude telefónico puede ser minimizado ofreciendo grados de protección frente a explotación de call forwarding y el paso de llamadas inter-troncales. El plan de numeración debe estar acorde a la política de seguridad y debe ser flexible. Por ejemplo, tal vez no todos los usuarios deben tener acceso a números pagados. También puede ser interesante implementar códigos de autenticación para llamadas a teléfonos móviles y larga distancia.
Es interesante agrupar estas (y muchas otras) recomendaciones de seguridad de telefonía IP de la siguiente forma:

Nivel 1
- Features adicionales en la solución sin costro extra.
- Overhead administrativo mínimo.
- Experiencia del usuario final no cambia.

Nivel 2
- Features adicionales pueden ser incluidos a bajo costo.
- Algo de overhead administrativo.
- Experiencia del usuario final puede cambiar.

Nivel 3
- Features avanzados pueden ser incluidos a alto costo.
- Costos operacionales y de implementación son superiores.
- Experiencia del usuario final es alterada.
- Feature avanzado puede impactar escalabilidad de la solución.

En la medida en que se va avanzando en nivel de seguridad, se avanza también en costo, complejidad, mano de obra y overhead administrativo. Posicionar la importancia de la seguridad de la telefonía IP dentro del espectro de aplicaciones de la red es vital para determinar una política consistente y sostenible en el tiempo.
La seguridad de la telefonía IP es un tema complejo, que abarca al usuario, a toda la infraestructura de red y a las aplicaciones. Si la red no es segura, tampoco lo será la telefonía IP. Como cualquier problema complejo, es más manejable si se abarca en fases, en módulos y con una estrategia simple pero clara, tal y como lo describía Sun Tzu en su excelente obra. ●

Más Info

En varias ediciones anteriores de NEX hemos desarrollado temas referidos a la telefonía IP, no duden en consultarlos si quieren ampliar lo visto en este artículo.
La edición #25 fue un especial dedicado a este tema con los artículos: "Telefonía IP, las cifras en Argentina", "IP Telephony: entendiendo sus tecnologías", "H323 vs. SIP Identity", "Más allá de la voz", "Live Communication Server 2005", "VoIP en Argentina" y"Telefonía IP entre diferentes fabricantes".
En NEX #27 se vio cómo es el mundo de la telefonía IP a través de un software de código libre: Asterisk.
La edición #28 contó con un artículo de Sergio Fernández, Gerente de Desarrollo de Negocios de Comunicaciones Unificadas de Cisco, sobre la atención al cliente y la telefonía IP.
Finalmente NEX #31 dio a conocer iptalk, una solución IP-PBX flexible que permite mantenerse al ritmo de las tecnologías de punta con características que transformarán completamente la manera en la cual su empresa se comunica.

Tributo a JIM GRAY

Conozca quién es Jim Gray, investigador de Microsoft y ganador del premio ACM Turing.

Jim Gray es investigador y manager del eScience Group de Microsoft Research. Sus principales intereses han estado focalizados en las bases de datos y los sistemas de procesamiento de transacciones (transaction processing systems), focalizándose en lograr que el uso de las computadoras para investigaciones científicas sea el más productivo posible. Su grupo trabaja en las áreas de astronomía, geografía, hidrología, oceanografía, biología y en salud.

Mantiene un gran interés en construir supercomputadoras reduciendo el costo de almacenamiento, procesamiento y networking, mediante el trabajo en la construcción de redes rápidas, grandes web servers con Cyber Bricks, y la construcción de un Server de almacenamiento de muy bajos costos y de alta performance. Jim también trabaja junto a la comunidad de astronomía para construir el World-Wide Telescope; y ayudó en las construcciones de bases de datos online como http://terraService.Net y http://skyserver.sdss.org. Cuando todos los datos del mundo de la astronomía estén en Internet y de forma accesible como una base de datos única y distribuida, Internet será el telescopio más grande del mundo.

Recientemente ha estado trabajando con la comunidad científica (Oceanografía, Hidrología, monitoreo ambiental, etc.) para construir una biblioteca digital que integre todos los libros de la comunidad científica. Es un investigador activo, además de ACM, NAE, NAS y Socio de AAAS. Recibió el ACM Turing Award en 1998 por su trabajo en la implementación de sistemas informáticos para el procesamiento de transacciones. Además editó una serie de libros sobre administración de información.

En la búsqueda

El sábado 28 de enero de 2007 Jim Gray, de 63 años, partió solo en su velero, llamado 'Tenacious', de la costa de San Francisco y desde ese día que no se sabe nada de su paradero ni de su embarcación. Jim había salido con destino a las islas Farallon, a unos 40 kilómetros al oeste del puente Golden Gate, de San Francisco, donde pensaba esparcir las cenizas de su madre.

Por tres días la Cost Guard de los Estados Unidos realizó una exhaustiva búsqueda desde la bahía de Monterey, al sur de San Francisco, hasta el estado de Oregón con un avión, un helicóptero y seis patrulleros. Luego de 100 horas y 75 personas participando del operativo, decidieron suspender la búsqueda al no tener ningún resultado. Sin embargo, sus familiares y amigos continuaron por su cuenta. Para esto se dispuso una página web www.helpfindjim.com en donde se publican las últimas novedades. Ante la falta de resultados positivos, amigos, colegas, empleados de Microsoft y familiares de Jim formaron el grupo “Friends of Jim” quienes junto a más de 6.000 voluntarios participan activamente en la búsqueda que incluye un análisis de las imágenes satelitales de la costa. Además, expandieron la búsqueda a la costa de México, basándose en un análisis de las corrientes oceánicas y estimando cuán lejos pudo haber llegado la embarcación de 12 metros desde el día de su desaparición. La iniciativa está basada en la más avanzada tecnología y consiste en la utilización de websites, blogs, software adhoc, y la reconfiguración de imágenes satelitales creadas por un equipo de ingenieros de Google, Amazon, Microsoft y la NASA. Los familiares, amigos y colegas de Jim han estado trabajando con expertos en computación para analizar las imágenes satelitales y aéreas. Gracias a los mapas por satélite de Google Earth examinaron más de 560.000 imágenes de tres satélites diferentes, cubriendo un total de 5.630 km2 de océano. Para esto contaron con la ayuda de Sergey Brin, cofundador del gigante de búsqueda por Internet, quien ofreció su ayuda, al igual que los empleados de la tienda de comercio electrónico Amazon.com. Sin embargo, y a pesar del gran esfuerzo, aún no hay noticias de Jim. ●



SU GENTE NECESITA INFORMACIÓN.
Y QUE NADIE MÁS TENGA ACCESO A ELLA.

Microsoft Forefront es una familia de productos de seguridad que cubre todas sus necesidades: desde el perímetro de su empresa, pasando por los servidores, hasta las estaciones de trabajo. Y sumándole la simplicidad en administración, instalación y monitoreo, se convierte en la opción más adecuada para llevar al máximo la eficiencia en la gestión de seguridad informática.

Para mayor información, ingrese a **www.microsoft.com/latam/forefront/** ó llámenos al **0800-999-4617.**

Microsoft® Internet Security & Acceleration Server 2006

Microsoft® Forefront™ Security for Exchange Server

Microsoft® Forefront™ Security for SharePoint™

Microsoft® Forefront™ Client Security

Microsoft® Forefront™



Autor: **Leonel Iván Saafigueroa**

Una Laptop por niño

One Laptop per Child (OLPC), es un proyecto humanitario sin fines de lucro, con el objetivo de crear a muy bajo costo una poderosa herramienta de aprendizaje para los niños. Analizamos su sistema operativo y le contamos qué encontramos.

El nacimiento de una gran idea

Nicholas Negroponte, científico estadounidense y profesor del Massachusetts Institute of Technology (MIT), es el responsable del proyecto que pretende producir computadoras portátiles a bajo costo. La idea fue presentada en el Foro Económico Mundial de Davos en 2005, con la intención de crearlas en un principio a 100 dólares (aunque por el momento su costo es de 150 dólares).

El mayor desafío fue reducir el precio de la pantalla, luego se eliminó todo lo innecesario de las

FOTO: (c) OLPC, http://wiki.laptop.org/go/B1_Pictures

portátiles que se venden hoy en día en el mercado. Negroponte argumenta que son pesadas y realizan las mismas funciones en nueve formas diferentes, sin contar costos como marketing y publicidad que hacen que el precio del producto final sea mucho más elevado.
La fundación OLPC intenta vender los ordenadores al por mayor, tratando directamente con los ministerios de Educación y, de esa forma, distribuirlas como si fueran libros de texto y que los niños puedan llevárselas a sus casas. Lo que se pretende es disminuir la brecha digital en los países menos desarrollados.
Actualmente la fundación OLPC cuenta con el apoyo de Advanced Micro Devices (AMD), Brightstar, Google, News Corporation, Nortel y Red Hat.

El Hardware del primer prototipo OLPC "Z0/B1"

Esta primera generación de máquinas cuenta con una novedosa pantalla dual con una resolución de 1200 x 900 a 200 dpi, que puede ser usada en blanco y negro en alta resolución a la luz del sol y en modo normal a todo color. Uno de los aspectos importantes es el modo de suspensión, cuando se apaga la CPU puede mantener el contenido del display ahorrando así energía.
En su interior vienen equipadas con un procesador de 500 mhz AMD y 128 MB de memoria DRAM, 500 MB de memoria Flash y tienen tres puertos USB.
Estos equipos no tienen disco rígido. A esto se debe el poco peso y poco consumo de energía. Aquellos que quieran más memoria, podrán tenerla pues en la parte inferior de la pantalla



se encuentra una ranura para agregar una memoria SD.
Incluye Wireless 802.11b/g que en un futuro soportará el mesh network (la capacidad de acoplarse a otros laptops cumpliendo la función de router). Cada uno de estos prototipos puede comunicarse con su vecino más cercano, creando una red ad hoc, o red de área local, y por supuesto permite también el acceso a Internet. Por fuera nos encontramos con un producto muy modular con forma de pequeño maletín. El display puede girar 180 grados, lo que brinda comodidad y la posibilidad de ocultar el teclado dejando solo el display. Incluye a sus costados parlantes, un pad y dos botones similares a una consola de juego, salida para auriculares, entrada de micrófono externo y webcam.

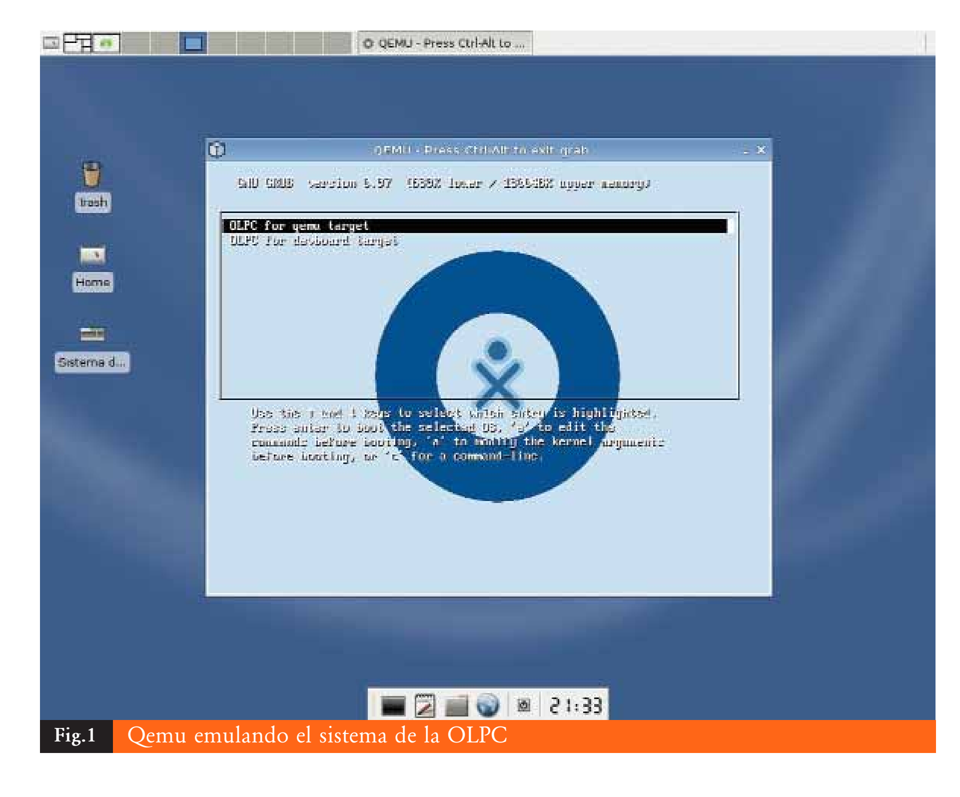


Fig.1 Qemu emulando el sistema de la OLPC

El teclado incluye las teclas de función modificadas para poder interactuar con la interfase "Sugar". Además está equipada con tres Touchpad: el central para manejar el puntero del mouse, y dos a los costados para ser utilizados en distintas aplicaciones de dibujo.
Todo el equipo está diseñado para resistir golpes, tiene un sistema de reposamiento adicional sobre todo en la parte del LCD, pero igual no deja de ser algo delicado.
La batería es un aspecto fundamental, en estos primeros prototipos tiene una duración de dos horas y están trabajando para que dure de dos a tres veces más, aunque ya están preparadas para soportar 2000 ciclos de carga (cuatro veces más que las laptops comerciales).

Probando el sistema operativo

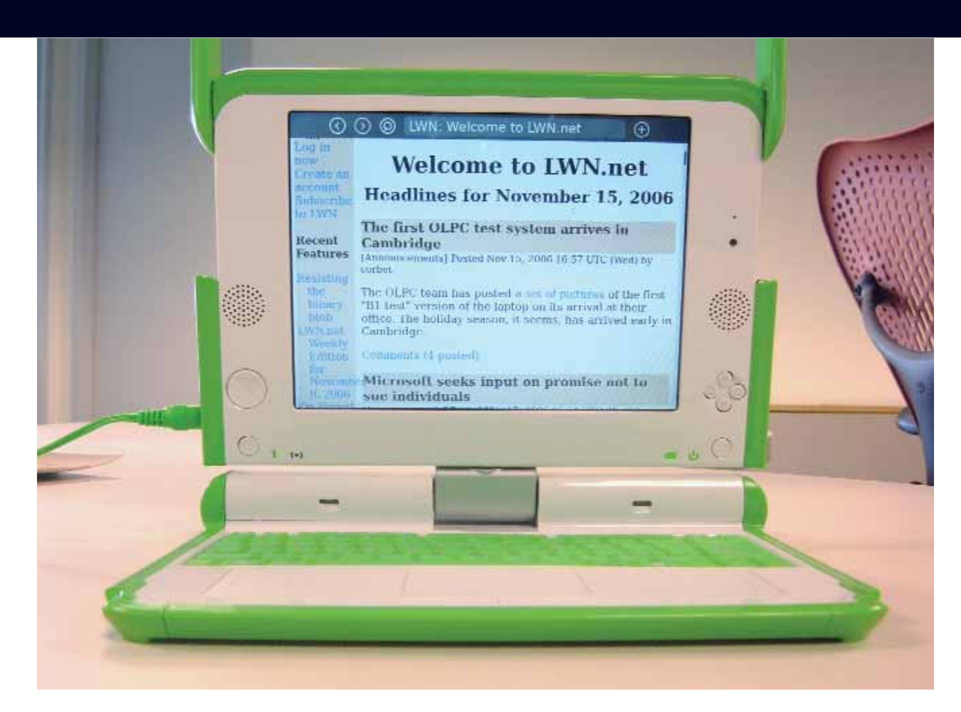
Hoy en día solo un número muy reducido de personas tienen acceso a la primera generación de estas laptops, la mayoría son desarrolladores. Pero al tratarse de software libre, tenemos la suerte de que todo el sistema (que aún está en desarrollo) puede ser descargado de Internet, y así emularlo en nuestra computadora. Aunque no es exactamente lo mismo, podemos darnos una idea de todo lo que pretende ofrecer esta innovadora herramienta.
Desde los servidores de Red Hat podemos descargar la imagen del sistema, también llamada "firmware", que actualmente se ejecuta en los prototipos reales.
(http://olpc.download.redhat.com/olpc/streams/development/)

La versión de la imagen utilizada en esta nota fue: olpc-redhat-stream-development-build-239-20070118_1355-ext3.img.bz2

En estos últimos meses las actualizaciones del sistema han sido casi constantes, aunque si descargamos cualquiera de las imágenes estables tendremos una idea de cómo es el sistema en estas laptops.
Luego hay varias formas de simular el sistema. En esta nota veremos cómo hacerlo con el emulador de código abierto "Qemu"; el mismo es multiplataforma y da la posibilidad tanto a usuarios de Windows, Mac OS X, o Gnu-Linux de tener éxito en estas pruebas. También es posible con los productos propietarios de VMware (ver wiki de OLPC para más detalles).

EMULANDO EN GNU-LINUX

1. Descargar el emulador desde (http://fabrice.bellard.free.fr/qemu/), en caso de usar alguna distribución como Gnu-Debian o similar, buscar en los repositorios, que posiblemente Qemu estará disponible. En Debian bastará con hacer un "apt-get install qemu".
2. Descomprimir la imagen del sistema del OLPC en un directorio.



3. Desde el mismo directorio ejecutar:
qemu -had olpc-redhat-stream-development-build-239-20070118_1355-ext3.img

EMULANDO EN WINDOWS

1. Descargar el emulador desde (www.h7.dion.ne.jp/~qemu-win/).
2. Descomprimir tanto el emulador como la imagen del sistema del OLPC en un mismo directorio.
3. Desde el mismo directorio ejecutar:
qemu -L . -hda olpc-redhat-stream-developent-build-239-20070118_1355-ext3.img

Tanto en Windows como en Gnu-Linux, el emulador abrirá una nueva ventana, y aparecerá rápidamente en pantalla OLPC 'XO'. En pocos segundos pasará al gestor de arranque Grub, en el que elegiremos 'OLPC for qemu target'. Luego veremos la típica secuencia de arranque de un linux Fedora, para terminar en una ventana de diálogo que nos preguntará por nuestro nickname (ingresar nuestro nombre para empezar a usar el sistema). Recuerden que presionando CTRL + ALT nos liberaremos de esa ventana para volver a controlar nuestro sistema operativo real.

Aplicaciones Incluidas

Una vez iniciado el sistema, navegar por la interfaz "Sugar" es relativamente sencillo. La metáfora Zoom muestra un ambiente en donde (de estar usando un prototipo real) podríamos visualizar a otros niños con sus laptops en un entorno que se denomina "neighborhood" (o "vecindad"). La interfaz permite además visualizar solo a aquellos del vecindario que consideramos "amigos", con los cuales se podrá trabajar en equipo.
Al mover el mouse a cualquiera de los extremos de la pantalla haremos aparecer el marco (o "frame"), desde el cual podremos escoger, por ejemplo, en el borde superior las visualizaciones de la metáfora Zoom. También los indicadores que nos muestran los programas que están siendo ejecutados en ese momento, y más arriba a la derecha el estado de la red a la que estemos suscriptos y el icono para apagar la laptop.
En el margen inferior aparecen todas las aplicaciones disponibles en el OLPC.
En esta emulación podremos probar programas para tener acceso al chateo entre las distintas laptops, navegador de Internet (Mozilla Firefox), procesador de texto (Abiword), cámara web, y algunos juegos de asociación de imágenes y sonidos para los más pequeños.
Actualmente se está probando la opción "compartir/no compartir", para tener la interactividad en cualquier trabajo realizado. Cada usuario será individualizado mediante un color único igual a cada instancia o actividad que desee compartir.

Conclusiones

Las primeras máquinas B1 llegaron a la argentina en enero y actualmente están siendo probadas por educ.ar. Se están haciendo muchas pruebas de ensayo y error, como también la primera capacitación para su uso. Solo el tiempo nos dirá si en verdad estas laptops son, como dicen sus creadores, "una ventana al mundo y una herramienta con la cual pensar, un camino para que los niños puedan aprender interactuando y explorando".

Aún es largo el camino que va del deseo a la realidad. Espero que los lectores se animen a emular el sistema operativo en sus computadoras y así probar todas las aplicaciones y seguir de cerca todo el desarrollo de un producto que aún tiene mucho por demostrar. ●

```
us=xx
[  119.137126] PIIX3: IDE controller at PCI slot 0000:00:01.1
[  119.175667] PIIX3: chipset revision 0
[  119.216148] PIIX3: not 100% native mode: will probe irqs later
[  119.257813]     ide0: BM-DMA at 0xc000-0xc007, BIOS settings: hda:pio, hdb:pio
[  119.300563]     ide1: BM-DMA at 0xc008-0xc00f, BIOS settings: hdc:pio, hdd:pio
[  119.705698] hda: QEMU HARDDISK, ATA DISK drive
[  120.456499] ide0 at 0x1f0-0x1f7,0x3f6 on irq 14
[  120.924424] hdc: QEMU CD-ROM, ATAPI CD/DVD-ROM drive
[  121.684980] ide1 at 0x170-0x177,0x376 on irq 15
[  121.795800] hda: max request size: 512KiB
[  121.832309] hda: 985057 sectors (504 MB) w/256KiB Cache, CHS=993/255/63, (U)DMA
[  121.875631] hda: cache flushes supported
[  121.917833]  hda: hda1
mounting /dev/root
lrwxrwxrwx 1 0 0 4 Jan 27 00:33 /dev/root -> hda1
[  122.394858] EXT3-fs: INFO: recovery required on readonly filesystem.
[  122.436661] EXT3-fs: write access will be enabled during recovery.
[  122.694690] kjournald starting.  Commit interval 5 seconds
[  122.733866] EXT3-fs: recovery complete.
[  122.778772] EXT3-fs: mounted filesystem with ordered data mode.
transfering control to /sbin/init
INIT: version 2.86 booting
                Welcome to Fedora Core
                Press 'I' to enter interactive startup.
Setting clock : Sat Jan 27 00:33:15 EST 2007               [  OK  ]
Starting udev:                                             [  OK  ]
Setting hostname localhost.localdomain:                    [  OK  ]
raidautorun: failed to open /dev/md0: No such device or address
_
```

Fig.1 El arranque del pequeño sistema Fedora del OLPC

Páginas de Internet

- Página oficial del proyecto.
http://www.laptop.org/
- Página con instrucciones para emular el sistema.
http://wiki.laptop.org/go/Home
- El software en desarrollo.
http://olpc.download.redhat.com/olpc/streams/development/
- Si eres un desarrollador no dudes en visitar esta pagina, aquí se reúnen los **posts de los desarrolladores y los voluntarios del OLPC**.
http://planet.laptop.org
- Página del emulador de código abierto Qemu.
http://fabrice.bellard.free.fr/qemu/

FOTO: (c) OLPC, http://wiki.laptop.org/go/B1_Pictures



IDC Argentina Business Intelligence & Business Performance Management Conference 2007

Jueves 19 de Abril de 2007
Hotel Hilton Buenos Aires,
Salón Buen Ayre, 2° piso

Patrocinadores Platinum:





Algo pasa en el Mundo de los Celulares



Ricardo D. Goldberger
Periodista Científico especializado en Informática y Nuevas Tecnologías

Mientras la mayor parte de los programadores y desarrolladores miran hacia el mundo informático (servidores, workstations, desktops), un grupo chico pero creciente observa lo que está pasando en el mundo de lo más pequeño: celulares y PDAs, y participa cada vez más. No hay que perderles pisada.

Estaba leyendo algunas estadísticas que Enrique Carrier (Carrier & Asoc.) escribió en su newsletter Comentarios. Las voy a reproducir textualmente para que puedan evaluar todo el alcance que tienen:
"Está claro que con la penetración actual de los celulares, del orden del 80%, no es mucho lo que se puede esperar en términos de crecimiento cuantitativo, o sea, más líneas. Así, a los operadores celulares les queda el camino cualitativo, es decir, lograr que suba el consumo por línea. Y este crecimiento no vendrá tanto de la gente hablando más sino del uso de los servicios que no son de voz".
"Esto se evidencia repasando las cifras del 2006. Durante el año pasado, las líneas crecieron un 50%, levemente por debajo de la facturación total. Hasta aquí, lineal. Sin embargo, las llamadas sólo crecieron un 32%. Esta diferencia entre el crecimiento de facturación y el de llamadas dan una pauta de que el celular es cada vez menos teléfono y cada vez más un dispositivo de funciones varias".
Luego de comentar que el 60 % de los usuarios lo usan más para mensajes de texto que para voz, Carrier afirma que "cobran relevancia otros negocios, como la descargas de ringtones y juegos o el uso del mail y de Internet móvil, que si bien en términos porcentuales no asombran, habida cuenta del tamaño de la base (32 millones de líneas), hablar de un 5% de usuarios equivale a 1,6 millones de personas. Así, un negocio que capte porcentajes de un dígito de la base total no es para nada desdeñable".
Y después de analizar el fenómeno de la participación de los televidentes en programas a través de los mensajes de texto (desde Call TV hasta Gran Hermano), Carrier concluye: "el celular presenta dos ventajas respecto de los medios de pago habitualmente utilizados en transacciones online, típicamente la tarjeta de crédito. Por un lado, aparece como el medio idóneo para realizar micropagos, es decir, por montos de centavos, terreno en el cual las tarjetas nunca pudieron hacer pie. Por el otro, tiene el gran atractivo de llegar a segmentos no bancarizados que no tienen otra alternativa simple de pago electrónico".
"De esta forma, el desarrollo del pago a través del celular permitiría ampliar el mercado de contenidos pagos, los cuales mayormente hoy se financian por abonos o por publicidad".
De lo que Carrier está hablando, en definitiva, es de la creciente demanda de servicios de programación para celulares o PDAs (o smartphones, blackberry's o palms... escrito así en minúsculas para significar genéricos), ya sea con los propios SDKs o mediante J2ME.
Hay tres vertientes desde las cuales abordar este fenómeno.
Por un lado, el de los servicios ya establecidos: plataformas de juegos y juegos, ingreso de llamadas para intervenir en concursos, sorteos o certámenes, delivery de información, facturación de todos estos servicios, etc. Todos estos sistemas necesitan mano de obra sumamente especializada cada vez en mayor demanda.
En una segunda instancia, está el desarrollo a medida. Tanto los teléfonos celulares como las PDAs (especialmente estas últimas) se han convertido en herramientas de trabajo para una multitud de tareas: desde el levantamiento de pedidos hasta el control de calidad de construcciones. GPS, WiFi, Bluetooth y otras tecnologías le han permitido a estos dispositivos reemplazar equipamiento más costoso como son las notebooks o las terminales de levantamiento de datos.
Como tercera vía, está el desarrollo de nuevos sistemas. Aquí se trata, además de creatividad, de encontrar un nuevo producto o servicio que pudiera venderse a las operadoras o a las compañías que se dedican a la provisión de contenidos.
Finalmente, el contexto: si bien tanto Windows como Linux están ganando cada vez más espacio, hasta ahora PalmOS y Symbian son los sistemas operativos predominantes. Y eso sin contar la diversidad de hardware, que hace necesarios ajustes a una misma aplicación no sólo entre distintas marcas sino también entre los modelos de una misma firma.
Fíjense si no hay como para estar atento. ●

Lo Nuevo Windows Server Update Services 3.0

Autor: **Alejandro Mazzitelli**
Microsoft Certified Professional

Recientemente Microsoft ha publicado un Release Candidate (beta próxima a salir) de WSUS 3. Debido a que los cambios son muchos e importantes, en esta nota le mostramos algunas de las nuevas características del producto.

Sin lugar a dudas Windows Server Update Services es un excelente producto para ahorrar nuestro tiempo al momento de aplicar las actualizaciones de los productos de Microsoft debido a la facilidad que presenta para instalarlos. Algo mucho mejor aún, es la tranquilidad de poseer toda nuestra infraestructura al día en materia de actualizaciones críticas de seguridad. Otra de las ventajas del producto es la reducción del consumo de ancho de banda de nuestra conexión a Internet debido a que solo realiza una descarga para luego distribuir los denominados "Fixes" (actualizaciones) por nuestra red interna.

Instalación

El asistente de instalación de WSUS 3 es muy sencillo de configurar pero para ello debemos contar con algunos requisitos mínimos:

- Windows Server 2003 Service Pack 1 o superior
- Microsoft Internet Information Server 6.0 o superior
- Background Intelligent Transfer service (BITS) 2.0
- Windows Installer 3.1
- Microsoft .Net Framework 2.0

Dependiendo del tamaño de nuestra infraestructura, WSUS 3 puede ser instalado utilizando algún servidor de SQL Server que ya poseamos en la empresa, o bien si lo utilizaremos en empresas donde no poseamos una licencia de SQL Server, WSUS 3 usa una versión reducida de SQL Server 2005 denominada Embebedd Edition, la cual es gratuita al igual que lo es WSUS.

Al finalizar la instalación, la nueva edición de WSUS incluye un nuevo asistente post-instalación el cual permite configurar básicamente nuestro servidor y dejarlo operativo para nuestra red.

Administración simplificada

Una de las grandes características que posee WSUS 3 en cuanto a su administración es la integración con MMC (Microsoft Management Console). Como viene sucediendo desde hace ya un tiempo, Microsoft está desarrollando todos sus nuevos productos para que puedan ser administrados desde una consola MMC. Este tipo de consola le simplifica mucho la tarea a cualquier administrador de red, ya que podremos administrar WSUS desde cualquier equipo remoto. Para ello, deberemos contar con MMC en su versión 3, la cual viene incluida solo si poseemos aplicado R2 de Windows Server 2003. Si nuestro sistema operativo es Windows Server 2003 SP1, tendremos que descargar desde la web de Microsoft dicha versión, cuyo link encontrarán al final de esta nota. Otro punto importante es que podemos administrar varios servidores de WSUS desde una misma consola y así poseer toda la administración centralizada, tal como podemos apreciar en la Figura 1.

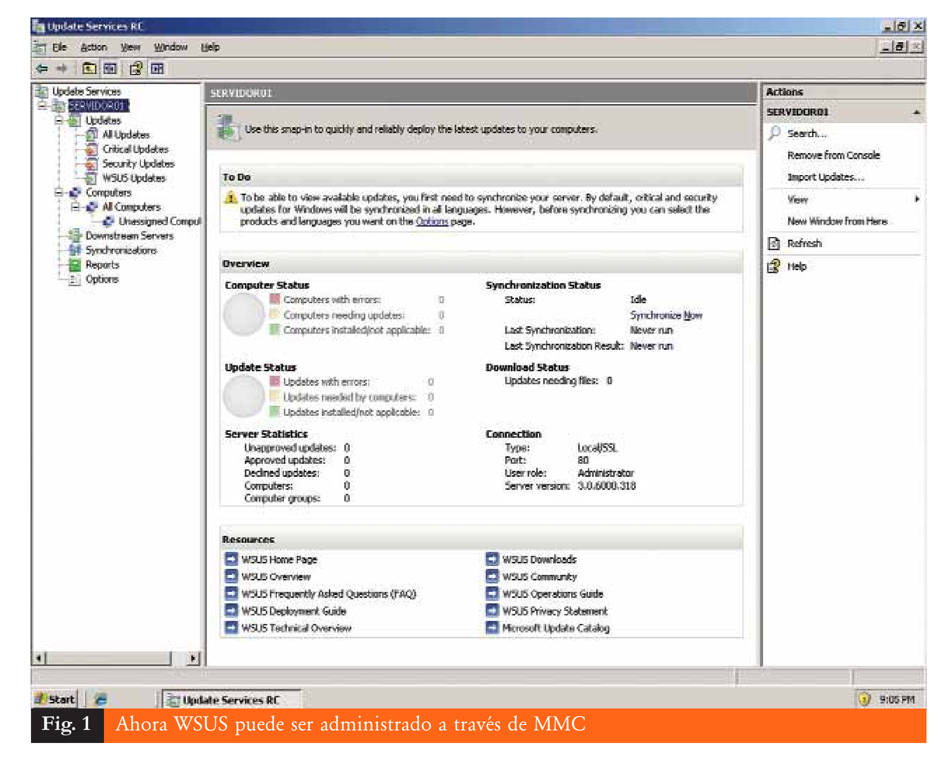


Fig. 1 Ahora WSUS puede ser administrado a través de MMC

Links y Lectura adicional

Descarga de WSUS 3.0 RC:
(una cuenta de Passport es requerida)
http://connect.microsoft.com/site/sitehome.aspx?SiteID=110

Descarga de Microsoft Management Console 3.0:
http://support.microsoft.com/kb/907265

Guía paso a paso de WSUS 3.0 (en inglés):
http://go.microsoft.com/fwlink/?LinkId=71190

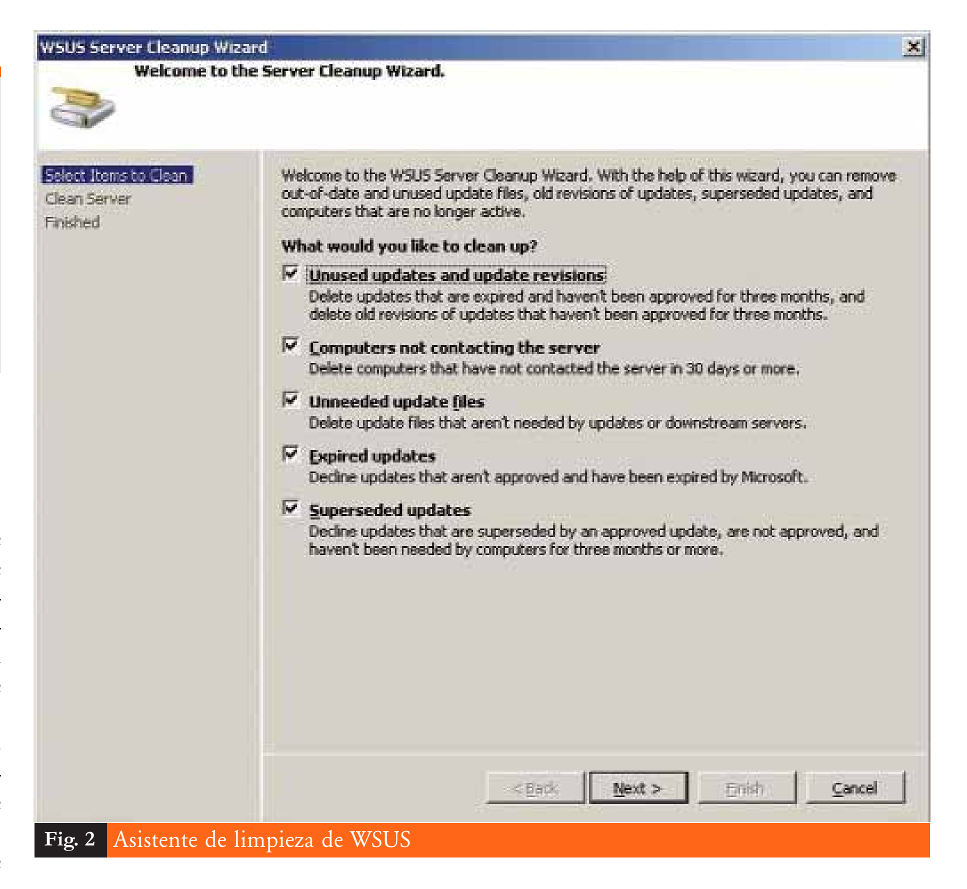


Fig. 2 Asistente de limpieza de WSUS

Reportes

La generación de reportes ha sido bastante mejorada en esta edición ya que permite generarlos desde cualquier vista donde se encuentren las actualizaciones, con un gran nivel de detalles, el cual podemos personalizar a gusto. Los reportes tienen la particularidad de ser exportados a Excel o bien a Adobe PDF. Para poder utilizar la generación de reportes es necesario contar con el componente Microsoft Report Viewer Redistributable 2005 que podemos descargar desde la web de Microsoft. Desde esta edición del producto es posible enviar mensajes alertando cuando se realiza una nueva sincronización de actualizaciones y también recibir reportes diarios o semanales.

Monitoreo

En cuanto al monitoreo, WSUS 3 reporta más detalladamente los sucesos en el Event Log. Para quien utilice Microsoft Operations Manager (MOM), Microsoft ya posee un paquete para monitorear los eventos generado por el servidor de WSUS.

Limpieza

Un nuevo asistente se suma a WSUS. Se trata de un asistente realmente muy útil al cual podremos indicarle qué tipo de objeto queremos "limpiar" del servidor. Es que a medida que utilizamos WSUS notaremos que nuestro servidor empieza a guardar información, la cual ocupa un espacio considerable dependiendo del espacio en disco con el que contemos. Este tipo de información en desuso pueden ser simplemente actualizaciones que desechamos o que no son utilizados luego de cierto período de tiempo, como así también equipos que ya no contactan al servidor, los cuales quedan registrados en la consola "Computers".

Actualizaciones soportadas

Los productos que son soportados por WSUS 3 para la descarga de sus actualizaciones son los siguientes:

- Windows 2000
- Windows XP
- Windows Vista
- Windows Server 2003
- Windows Small Business Server 2003
- Exchange Server 2000
- Exchange Server 2003
- SQL Server
- SQL Server 2005
- Office XP
- Office 2003
- Microsoft ISA Server 2004
- Microsoft Data Protection Manager
- Microsoft ForeFront
- Windows Live
- Windows Defender

WSUS 3.0 puede ser utilizado con Windows Server "Longhorn", la próxima edición de Windows para servidores. Para ello, algunos de los componentes requeridos ya vienen incluidos con el sistema operativo pero no activados por defecto como es el caso de Internet Information Server 7.0 (IIS 7). Es que a diferencia de su antecesor, debemos poseer algunos de sus componentes instalados: IIS Metabase Compatibility, Management Compatibility, Windows Authentication y ASP.NET.

Acerca del Autor

Alejandro Mazzitelli es Consultor en tecnologías Microsoft en TPS SA. Colaborador de comunidades dedicadas a tecnologías Microsoft tales como GLUE. Recientemente obtuvo la certificación de Microsoft Certified Professional orientado a MCSE. También posee la certificación en Implementación de Microsoft Dynamics CRM 3.0. Adicionalmente posee su blog personal en la siguiente URL: *http://www.mazzitelli.org*

Actualizando a WSUS 3.0

Si ya poseemos WSUS 2.0 instalado es bueno saber que podemos actualizarlo a WSUS 3. En este caso tenemos que actualizar nuestro servidor principal de WSUS y luego seguir con los siguientes en caso de que nuestra infraestructura posea más de uno. Antes de realizar una implementación con varios servidores debemos saber que WSUS 2 puede sincronizar datos desde un servidor WSUS 3 pero un servidor WSUS 3 no puede sincronizar datos desde un servidor WSUS 2.

Conclusión

Teniendo en cuenta las características de su antecesor, la nueva edición WSUS 3 incluye muchos cambios los cuales hemos cubierto en este artículo aunque no están todos, y que de acuerdo al uso y/o importancia que tenga este servicio en su infraestructura, estoy seguro de que una migración a corto plazo ya la tiene casi decidida. Les recuerdo que el producto aún está en desarrollo y algunas de las características pueden ser cambiadas en su versión final, por lo cual también es importante instalarlo en un ambiente de laboratorio. ●

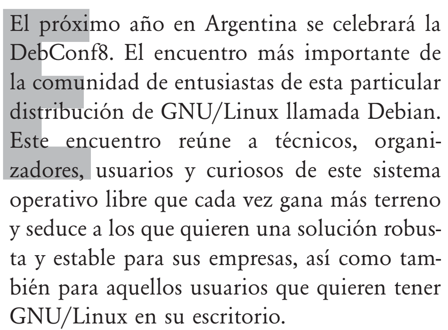
DebConf
En Argentina



Conozca todo sobre la conferencia más grande de usuarios de Debian que en 2008 estará en nuestro país.

debian

Autor: **Federico Nan** | Socio Gerente | **Nantec.net**



El próximo año en Argentina se celebrará la DebConf8. El encuentro más importante de la comunidad de entusiastas de esta particular distribución de GNU/Linux llamada Debian. Este encuentro reúne a técnicos, organizadores, usuarios y curiosos de este sistema operativo libre que cada vez gana más terreno y seduce a los que quieren una solución robusta y estable para sus empresas, así como también para aquellos usuarios que quieren tener GNU/Linux en su escritorio.

Debian se destaca por ser una de las distribuciones más antiguas de GNU/Linux, que mantiene el espíritu original de Unix y la filosofía del software libre. Existen varias distribuciones que se basaron en Debian para crearse. Ubuntu, por ejemplo, es una de las distros más usada para entornos de escritorio por su facilidad de uso, estabilidad y seguridad.

En el ambiente de servidores, Debian se destaca por ser un sistema confiable, con más de 15.000 paquetes (programas) precompilados listos para instalar. Es seguro y cada vez más fácil de manejar. Soporta la más variada línea de procesadores, que van desde el X86 hasta la línea Mainframe IBM 390.

La empresa HP recientemente reconoció a Debian como una de las distribuciones GNU/Linux soportadas por sus servidores Proliant y Blade.

En Argentina centros de capacitación en GNU/Linux migraron sus plataformas de enseñanza a Debian. Otros centros como CentralTech mantuvieron la línea usando Debian como soporte de enseñanza desde hace ya varios años.

Sobre el encuentro

El primer encuentro se llevó a cabo en Bordeaux, Francia, donde participaron alrededor de 30 entusiastas. Para la DebConf de Argentina se esperan más de 400 participantes. La conferencia se llevará a cabo en Mar del Plata y tendrá una duración de dos semanas. El evento va a estar dividido en tres etapas:

- **Debian Conference:** donde los mejores desarrolladores tienen su espacio de discusión técnica.

- **Debian Camp:** un espacio de encuentro para los diferentes grupos de desarrollo de Debian.

- **Debian Day:** dedicado a los entusiastas y visitantes. El Debian Day propone conocer este Software y, por sobre todo, esta maravillosa comunidad y su filosofía.

Lo que vale la pena recalcar es que la participación a este evento es totalmente gratuita.

Este año la DebConf se va a realizar en Edimburgo, Escocia. Si quieren tener más información sobre este evento pueden visitar http://debconf7.debconf.org o el sitio oficial de Debian http://www.debian.org.

En mi opinión este evento internacional que el año próximo elije Argentina para desarrollarse no tiene que pasar desapercibido para los entusiastas del Software libre más allá de la distribución que utilicen actualmente.

Un selecto grupo de usuarios Argentinos de Debian están organizando el evento para el año próximo, en busca de lugares y sponsors. Pueden visitar http://wiki.debconf.org/wiki/Argentina/Mar_del_Plata para obtener más información y si se animan -participar de este maravilloso encuentro! ●





Postfix al descubierto Parte 3

Configuración Avanzada, Antivirus y Antispam.

Autor: **Federico Nan** | Socio Gerente| **Nantec.net**

En los capítulos anteriores vimos cómo funciona Postfix y cómo configurarlo para tener un servidor de correo básico. En esta última entrega, nos enfocaremos en una configuración más avanzada, ocupándonos de la autenticación de usuarios y el cifrado del canal de datos por donde enviamos los mails. También incluiremos un servidor de Antivirus y Antispam. Manos a la obra…

Lo primero que tenemos que hacer es asegurar nuestro servidor de correo. Para esta tarea vamos a utilizar TLS (Transport Layer Security). TLS es un protocolo que permite encriptar un canal de comunicación de datos usando una infraestructura de claves públicas (ver recuadro "Más información"). En nuestro caso, las claves PKI las vamos a generar nosotros mismos, lo cual es una solución rápida y sin costos. Configurar las claves de TLS nos trae una pequeña pérdida de performance en los MUA (Mail User Agent) de Microsoft, ya que cada vez que el usuario abra el programa para revisar el correo, el MUA nos pedirá la aceptación del certificado que nos permite encriptar el canal de comunicación. Si no cerramos el MUA, este chequeo no se realiza hasta que el mismo se reinicie.

Podemos optar por obtener un certificado de alguna entidad certificante, pero en éste caso, tenemos que evaluar el costo de la compra del certificado.

Una vez que el MUA autentica y acepta el certificado, la comunicación SMTP estará encriptada, lo que nos da la seguridad de que nuestro correo llega a destino para ser solo leído por la persona a quien le mandamos la información y que no hay ninguna pérdida en el camino.

Son pocas las empresas que tienen en cuenta este paso de cifrado de las comunicaciones SMTP. Como saben, el correo actualmente es un servicio fundamental en nuestra estructura IT, y el protocolo SMTP no quedó a la altura de las circunstancias, por eso, esta alternativa de cifrado debería convertirse en un estándar de aplicación para los administradores de servidores de correo.

Con esta implementación podemos asegurarnos de que los mails que los usuarios manden a nuestro servidor llegarán seguros. También podemos configurar el MTA para que intente cifrar conexiones con otros MTA; pero en la práctica es difícil de implementar porque, como dije antes, muchos de los servidores no vienen con esta opción.

No todo es el SMTP, también tenemos que encargarnos de segurizar las conexiones POP3 e IMAP. En nuestro caso vamos a utilizar el programa Cyrus conectado a una base de datos de SASL (Simple Authentication and Security Layer) llamada SASLDB (ver recuadro "Más información").

Con Cyrus nos encargaremos de gestionar los usuarios del servidor de correo, como así también, de proveer el servicio de conexión IMAP/POP3.

Otra de las tareas de Cyrus, junto con SASL, es la de autenticar los usuarios para el envío de correo mediante SMTP AUTH usando contraseñas cifradas.

De esta manera el servidor queda cerrado aceptando el RELAY solo a nuestros usuarios autenticados.

Para que todo esto se convierta en realidad y podamos completar la instalación de un verdadero servidor de correo, vamos a ejecutar, a modo de ejemplo, algunos pasos para tener una idea más clara de la implementación.

Primero bajamos los programas necesarios para la implementación. En mi caso con Debian esta tarea resulta sencilla:

```
apt-get install libsasl2 sasl2-bin libsasl2-modules cyrus21-admin
cyrus21-common cyrus21-doc cyrus21-imapd
```

Una vez lista la instalación, modificamos los archivos de SASL para que lea la base de datos SASLDB, que es la que nos interesa e instalamos. Editamos el fichero */etc/default/saslauthd* y modificamos el parámetro *MECHANISMS:*

```
START=yes
MECHANISMS="sasldb"
```

Luego reiniciamos el servicio:

```
/etc/init.d/saslauthd restart
```

¡Listo! Ahora podemos crear los usuarios en la base de datos de SASL con los siguientes comandos:

```
saslpasswd2 -c cyrus
```

(este usuario debemos crearlo para que cyrus

pueda administrar sus usuarios)

```
saslpasswd2 -c prueba
```

El siguiente paso es crear los buzones de correo para el usuario Federico. Para esta tarea usamos el programa cyradmin:

```
cyradm --user cyrus localhost
```

Una vez dentro de la consola de cyradmin, creamos el mailbox del usuario. Aquí podemos setear las quotas, las carpetas compartidas, listas y eliminar usuarios entre otras cosas:

```
cm user.prueba
```

En la figura 1 podemos ver los pasos realizados. En la configuración de Postfix (main.cf) tendremos que cambiar unos parámetros para que el transporte de usuarios lo autentique contra Cyrus y no con su base actual (la que configuramos en los capítulos anteriores). Para eso vamos a agregar:

```
local_recipient_maps =
mailbox_transport =
lmtp:unix:/var/run/cyrus/socket/lmtp
```

En este paso vamos a agregar la autenticación de usuarios (SMTP AUTH). Tenemos que agregar al main.cf las siguientes líneas:

```
smtp_sasl_auth_enable = no
    smtpd_sasl_auth_enable = yes
    smtpd_sasl_local_domain = dominio.com
    smtpd_recipient_restrictions =
        permit_mynetworks,
        permit_sasl_authenticated,
        reject_unauth_destination
    smtpd_sasl_security_options = noanonymous
```

De esta manera nos aseguramos que los usuarios que no se autentiquen no podrán enviar correo a través de nuestro servidor.

Para que Postfix pueda cifrar la conexión SMTP tenemos que instalar el paquete OPEN SSL para crear los certificados; luego, agregar unas líneas como las que detallo a continuación, al main.cf:

```
smtpd_use_tls = yes
# smtpd_tls_auth_only = yes
smtpd_tls_key_file =
/etc/postfix/ssl/newreq.pem
smtpd_tls_cert_file =
/etc/postfix/ssl/newcert.pem
smtpd_tls_CAfile =
/etc/postfix/ssl/cacert.pem

smtpd_tls_loglevel = 3
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout =
3600s
tls_random_source = dev:/dev/urandom
```

Este paso puede volverse complicado, ya que Postfix corre en un ambiente enjaulado y necesita que todos los archivos a los que tiene que acceder estén dentro de su jaula donde tiene permisos. Hay mucha información en Internet sobre cómo hacer que Postfix lea estos archivos. Luego de todos estos cambios, el archivo main.cf quedaría como la imagen 3. Para probar si los cambios que hicimos tuvieron efecto, tanto en este como en cualquier servidor de correo, podemos volver a utilizar telnet.

```
debian:~# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.localdomain.
Escape character is '^]'.
220 debian.nantec.net ESMTP Postfix (Debian/GNU)
ehlo debian.nantec.net
250-debian.nantec.net
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH LOGIN PLAIN
250 8BITMIME
AUTH PLAIN ZmVkZXJpY28AZmVkZXJpY28AZXVyZWth
235 Authentication successful
STARTTLS
220 Ready to start TLS
mail from:federico
Connection closed by foreign host.
debian:~# _
```

Fig. 2

Filtrar Correo

Para filtrar el correo en Postfix vamos a utilizar una herramienta llamada Amavisd-new (ver "Más información"). Ésta es la encargada de comunicar a Postfix con el Antispam y el antivirus. La comunicación puede establecerse mediante LMTP (Local Mail Transfer Protocol) o ESMTP (Extended Simple Mail Transfer Protocol). También hay otros programas para realizar comunicaciones, pero éstos son los más usados por su velocidad y estabilidad. Amavisd-new levanta un servidor SMTP que cumple con el RFC 2821 o un servidor LMTP que cumple con el RFC 2033.

Cuando la cantidad de usuarios es importante, por ejemplo más de 1.000, lo ideal es montar el servidor de Amavisd-new en otro equipo para que el escaneo de mails no produzca una pérdida de performance en la entrega de correo. El servidor de Antispam (SpamAssassin) suele ocupar muchos recursos para llevar a cabo su tarea de escaneado de mails.

Para comenzar el filtrado de correos, primero tenemos que configurar el Amavisd-new, que activa el filtro Antispam, pero también podemos configurar un antivirus, como por ejemplo el Clamav, que es Open Source.

En el caso del Antispam, Amavid-new se encarga de tomar el módulo de Mail: SpamAssassin de Perl para realizar las tareas de filtrado. Por cada mail recibido se llamará al modulo de SA (SpamAssassin) para que realice el escaneo.

El SA escanea el mensaje y también chequea on-line en listas de correo negras. Utiliza pruebas heurísticas para escanear el cuerpo y encabezado y así detectar el Spam. También contamos con una herramienta de Auto Learning, pudiendo indicarle al SA que aprenda de correos que nosotros le indicamos. Podemos educarlo indicándole cuáles son Spam y cuáles no. También tiene la opción de crear listas negras y listas blancas de correo, así como también omitir dominios o usuarios

```
debian:~# saslpasswd2 -c

This product includes software developed by Computing Services
at Carnegie Mellon University (http://www.cmu.edu/computing/).

saslpasswd2: usage: saslpasswd2 [-v] [-c [-p] [-n]] [-d] [-a appname] [-f sasldb
] [-u DOM] userid
        -p      pipe mode -- no prompt, password read on stdin
        -c      create -- ask mechs to create the account
        -d      disable -- ask mechs to disable/delete the account
        -n      no userPassword -- don't set plaintext userPassword property
                        (only set mechanism-specific secrets)
        -f sasldb       use given file as sasldb
        -a appname      use appname as application name
        -u DOM  use DOM for user domain
        -v      print version numbers and exit
debian:~# saslpasswd2 -c prueba
Password:
Again (for verification):
debian:~# cyradm --user cyrus localhost
IMAP Password:
              localhost.localdomain> cm user.prueba
localhost.localdomain> lm
user.federico (\HasNoChildren)  user.prueba (\HasNoChildren)
localhost.localdomain> quit_
```

Fig. 1

Más Información

Configurar Postfix es una tarea sencilla siempre y cuando elijan consultar en las páginas oficiales de cada programa. Recuerden que cuentan con el apoyo de toda una comunidad, que de seguro volcó en listas de correo sus experiencias con ésta maravillosa herramienta de correo.

- **http://www.postfix.org**
- **http://cyrusimap.web.cmu.edu/**
- **http://asg.web.cmu.edu/sasl/**
- **http://spamassassin.apache.org/**
- **http://www.ijs.si/software/amavisd/**
- **http://www.clamav.net/**
- **http://es.wikipedia.org/wiki/SSL**

```
relayhost =
mynetworks = 127.0.0.0/8
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
local_recipient_maps =
mailbox_transport = lmtp:unix:/var/run/cyrus/socket/lmtp
smtp_sasl_auth_enable = no
smtpd_sasl_auth_enable = yes
smtpd_sasl_local_domain =
smtpd_recipient_restrictions =
   permit_mynetworks,
   permit_sasl_authenticated,
   reject_unauth_destination
smtpd_sasl_security_options = noanonymous
smtpd_use_tls = yes
# smtpd_tls_auth_only = yes
smtpd_tls_key_file = /etc/postfix/ssl/newreq.pem
smtpd_tls_cert_file = /etc/postfix/ssl/newcert.pem
smtpd_tls_CAfile = /etc/postfix/ssl/cacert.pem
smtpd_tls_loglevel = 3
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom
                                                          1,1           Todo
```

Fig. 3

específicos del escaneado.
EL SA es una de las herramientas AntiSpam más utilizadas en Apliances y Servidores.
Es importante mantener instalada la última versión de SA, ya que generalmente cuentan con nuevas herramientas de filtrado.
Las configuración general de filtrado la hacemos con el Amavisd-new en su archivo de configuración en /etc/amavisd.conf.
El SA trabaja dando una puntuación por cada elemento de concordancia encontrado; esos puntos (hits) se van sumando y nosotros podemos configurar en el amavisd-new el tope de puntuación que un mail puede tener. Cuando llega al límite, el amavisd-new puede ejecutar varias acciones, mandar un mail al emisor del mensaje, al destinatario, borrar el mensaje o marcarlo en el asunto como SPAM, entre otras.
La puntuación normal que podemos dar a un mensaje como tope es de 5 hits. Pero esto depende mucho de la empresa y la política de filtrado que utilice. Recuerden que cuanto menos hits pongamos como tope, más Spam va a filtrar, pero cabe la posibilidad de encontrar falsos positivos y estar filtrando correo que no es Spam. Esto les puede traer muchos dolores de cabeza como administradores de red. Por eso es importante sólo marcar (durante uno o dos meses) los mensajes como SPAM, y estudiar bien cada caso; luego enseñarle al SA qué es Spam y qué no. Les puedo asegurar que después de finalizar el estudio van a estar filtrando el 98 por ciento del Spam.

Concluyendo

En este último capítulo dimos una vista general en configuraciones avanzadas en Postfix. Ahora tienen una idea de cómo segurizar la autenticación de usuarios, el canal de transporte y también filtrar el Spam. No es una tarea sencilla, pero les aseguro que una vez que lo tengan funcionando -no van a arrepentirse!●

UADE

Conozca el departamento de sistemas y las investigaciones de una de las Universidades más tradicionales del país.

La Universidad Argentina de la Empresa (UADE) es una institución con más de 40 años de actividad en la enseñanza universitaria. Si bien es una institución que nació y se desarrolla desde una perspectiva netamente empresarial, su Departamento de Tecnología Informática lleva adelante algunas de las investigaciones más interesantes dentro del campo IT.

El Departamento de Tecnología Informática, a cargo del Ingeniero Alejo Fedor Rubin Aymá, tiene la responsabilidad del dictado de todos los cursos relacionados con el área de Informática y Computación que se dictan en la Universidad. Esto incluye no solamente a los cursos dictados para las carreras de Ingeniería y Licenciatura en Informática, sino también los de Programación y Sistemas para las restantes carreras de la Facultad de Ingeniería, y los cursos de microinformática para las carreras de las otras Facultades de la Universidad.

En particular, los cursos del departamento están agrupados en las siguientes áreas temáticas:
- Programación
- Sistemas de Información
- Microinformática y aplicativos específicos
- Tecnologías informáticas
- Gestión de Sistemas y de la Información

Con respecto a la *gestión*, tanto Rubin Aymá como Javier Zuñiga, Director de Ingeniería en Informática de la UADE, coinciden en que es el diferencial que brinda la institución a sus alumnos: "no solo es un tema de software y hardware sino también cómo se aplica y con casos de análisis reales", explican.

Hoy en día la facultad tiene aproximadamente 1.600 alumnos cursando la Licenciatura en



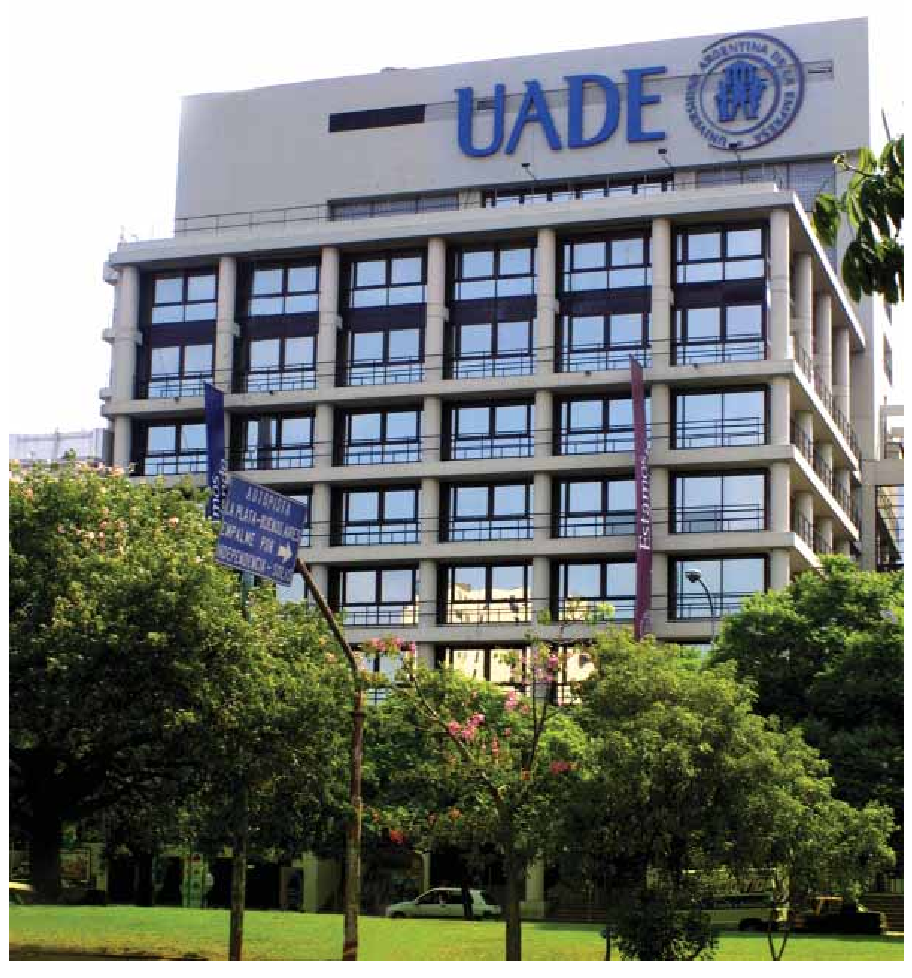
Vanguardia y Trayectoria



CaFeCONF

Como desde hace 3 años, en 2006 se realizaron en el predio de la Universidad Argentina de la Empresa las 5tas Conferencias Abiertas de GNU/Linux y Software Libre (CaFeCONF), organizadas por CaFeLUG (Capital Federal Linux User Group) que tienen por objetivo la difusión del Software libre a la mayor cantidad de gente posible.
Más de cientos de personas se acercaron a la UADE para participar de las más de 70 conferencias, talleres y tutoriales. Entre los expertos que formaron parte del evento se encontraron Alex Martelli y Anne Ravenscroft, de la Python Software Foundation, y Martin Langhoff, del proyecto Moodle y Catalyst de Nueva Zelanda.

El evento fue declarado, por segundo año consecutivo, de Interés Cultural por la Legislatura de la Ciudad Autónoma de Buenos Aires.



Informática o la carrera de Ingeniería Informática. Sin embargo, las empresas viven una realidad en la que no pueden esperar los tiempos de la enseñanza para contar con los profesionales. Para estos casos la UADE da la posibilidad a sus alumnos de cursar diferentes especializaciones para anticipar lo que más adelante van a ver en la carrera. “Brindamos cursos de .Net, de Redes y de programación en JAVA para que los alumnos tengan una salida laboral más inmediata y, así, colaborar con el mercado empresarial, ya que estos temas se ven más adelante en la carrera; de esta forma los alumnos pueden ir adquiriendo una experiencia laboral mientras estudian”, explica Zuñiga.

Además, la Facultad realiza una campaña activa brindando información sobre sus carreras a los alumnos de los últimos años del colegio secundario. Se dictan clases abiertas donde se invita a los alumnos del secundario con una temática teórica pero a la vez práctica. “No solo conocen un tema específico sino que además vienen y juegan, tocan, arman y desarman, y de esta forma pueden aplicar los conocimientos teóricos que recién se vieron”, explica Rubin Aymá.

El Departamento también colabora en la coordinación y uso de los Laboratorios de Informática, conjuntamente con la Dirección de Laboratorios. La casi totalidad de los cursos dictados por el Departamento incluyen la realización de prácticas en estos laboratorios, a los fines de que los alumnos adquieran la experiencia práctica necesaria para desempeñarse profesionalmente.

Son en total 11 laboratorios de informática equipados con 300 PC’s, más un laboratorio específico de Mac, otro de telecomunicaciones (donde se ve el tema de redes) y uno de robótica, entre otros. En este último en 2006 se desarrolló un robot altamente sofisticado que se maneja a través de un joystick, con conexión Wi-Fi, cámara que recibe y emite imágenes, un brazo articulado y un sensor GPS para poder ubicarlo. “Lo que vale recalcar de este logro es que fue un trabajo en conjunto, multidisciplinario, con una integración de varias carreras, y el proyecto no queda cerrado, sino que la condición sine qua non es que otro grupo le pueda realizar modificaciones y de esta forma mejorarlo”, comenta Zuñiga.

El cuerpo docente del departamento está conformado en su mayoría por docentes con experiencia profesional, que se desempeñan en empresas de primera línea. Esto asegura no sólo una fuerte relación con estas empresas, sino también la directa aplicabilidad de los conceptos enseñados en el campo laboral.

Por último, el Departamento realiza investigaciones en el área Informática, en particular en el área de Desarrollo de Sistemas Confiables. Estas investigaciones son desarrolladas por investigadores de la Universidad, que también dictan clases y dirigen trabajos finales en la Facultad de Ingeniería. ●

Los responsables

Alejo Fedor Rubin Aymá se graduó como Ingeniero en Electrónica en la Universidad Tecnológica Nacional, Facultad Regional Bs. As. en 1982. Actualmente es Profesor titular y Director del Departamento de Tecnología Informática de la Facultad de Ingeniería de la Universidad Argentina de la Empresa desde 2003.
Javier Zuñiga es Licenciado en Informática de UADE, Magister en Ing. de Software de la UNLP, MBA de EDDE y es Director de carrera de Ingeniería Informática y profesor adjunto ordinario exclusivo en las materias de Análisis de Sistemas, Ciclo de Vida de Sistemas, Seminario de integración profesional II e Ingeniería de software I.



BREVES

Google Docs & Spreadsheets

Google presentó una solución gratuita para manejar documentos online en forma colaborativa y en español. Google Docs & Spreadsheets es un procesador online de texto y hojas de cálculo que permite crear, editar y compartir este tipo de documentos.
Con esta solución Google resuelve el problema que implicaba trabajar con documentos a través de diversas personas, versiones, ubicaciones y usos horarios.
Además, Google brinda a los usuarios de habla hispana la posibilidad de acceder en su idioma a esta solución a través de la barra de herramientas Google Toolbar 3 para Firefox, lo que permite ahorrar tiempo y acceder automáticamente a los documentos y hojas de cálculos en este explorador.
Con esta solución los usuarios podrán crear documentos de texto y hojas de cálculo y manejarlas online en cualquier momento y lugar, compartir estos documentos con otras personas y especificar quién puede modificarlos y quién no, colaborar con el trabajo de otros en tiempo real, importar sus documentos de texto y hojas de cálculo y publicar el trabajo realizado en un Blog o en una página HTML.
Google Docs & Spreadsheets está actualmente en su versión beta, disponible en forma gratuita y abierta para todos. Para conocer mejor el producto puede ingresar a http://docs.google.com. ●

Impulso en la investigación tecnológica argentina

El presidente de la Nación, Néstor Kirchner, firmó el decreto de creación de la fundación Sadosky cuya composición es mixta dada la participación del Ministerio de Educación, Ciencia y Tecnología de la Nación, el Ministerio de Economía de la Nación, Universidades Nacionales, de empresas y de entidades vinculadas a las tecnologías de la información, con una participación activa de la Cámara de Empresas de Software y Servicios Informáticos (CESSI).
La Fundación Sadosky tiene por objetivo brindar valor agregado a la producción científica tecnológica argentina y competitividad a las empresas tecnológicas de nuestro país para convertir a la Argentina en un país líder entre los no centrales en 2014.
La fundación lleva el nombre de Manuel Sadosky, (1914-2005), Doctor en Ciencias Físicas y Matemáticas en la Facultad de Ciencias Exactas de la Universidad de Buenos Aires (UBA), fue Vicedecano de esa Facultad de 1958 a 1966, creó el Instituto de Cálculo y trajo a la Argentina, con el apoyo de Bernardo Houssay, la primer gran computadora del país y de América Latina "Clementina". ●



Turing Award

Primera vez que es ganado por una Mujer

Fraces Allen, quien fue una científica de IBM, recibirá en junio el Turing Award 2006 por un programa de optimización del trabajo, según anunció la Association for Computing Machinery. Por este premio recibirá 100.000 dólares y el reconocimiento mundial de la industria del IT.
Allen es conocida por el desarrollo de Ptran (Parallel Translation), un método específico para correr un programa sobre múltiples procesadores para mejorar la velocidad y la eficiencia. Además, hizo un master en matemáticas en la Universidad de Michigan y recibió un título en educación de la Albany State Teachers College.
En 1957 se unió al equipo de IBM para enseñar el programa de lenguaje Fortran (Formula Translation). Desde ahí continuó con el desarrollo de un programa de optimización y con Ptran.
Su trabajo ayudó a la fundación del sistema de high-speed computing usado en la actualidad para el pronóstico del clima, el análisis del ADN y el análisis de la seguridad nacional. ●

BEA Systems y su servicios de consultoría

BEA Systems, compañía dedicada al software de infraestructura corporativa, anunció una nueva suite de servicios de educación y consultoría en SOA especialmente creada para ejecutivos de tecnología. Esta suite tiene como objetivo brindar herramientas a los ejecutivos para invertir en SOA como un camino para agregar valor a su negocio.
SOA para Ejecutivos ha sido diseñada para demostrar los beneficios en gobernabilidad y organización de sistemas de las inversiones realizadas en SOA. Para esto brinda específicamente servicios de Consultoría y Educación.
Para más información sobre las soluciones de SOA que provee BEA, visite: www.bea.com/services. ●

Humor - *Por Severi*







Roberto Coceres, jugador del Nationwide Tour. Campeonato Argentino de Profesionales, San Eliseo 2005.





Inscríbase en alguna de las clínicas y/o salidas que se realizarán en forma exclusiva para CEOS y CIOS.

www.mundodelsoporte.com



El Mundo del Soporte

A Member of SupportLand Network